Hewlett Packard Enterprise

HPE FlexNetwork MSR1000, MSR2000, MSR3000 and MSR4000 Router Series

FIPS 140-2 Non-Proprietary Security Policy

Security Level 2 Validation

Version 1.00

June 2017

Revision Record

Date	Revision Version	Change Description	Author
2017-01-12	1.00	Initial version	HPE

Table of Contents

TABLE OF TABLES

TABLE OF FIGURES

FIPS 140-2 Non-Proprietary Security Policy for the HPE FlexNetwork Routers

Keywords: Security Policy, CSP, Roles, Service, Cryptographic Module

List of abbreviations:

Abbreviation	Full spelling
AAA	Authentication, Authorization, and Accounting
AES	Advanced Encryption Standard
CF	Compact Flash
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
DES	Data Encryption Standard
DOA	Dead on arrival
FCoE	Fibre Channel over Ethernet
FIPS	Federal Information Processing Standard
HMAC	Hash-based Message Authentication Code
HTTP	Hyper Text Transfer Protocol
IRF	Intelligent Resilient Framework
KAT	Known Answer Test
LED	Light Emitting Diode
LPU	Line Processing Unit
MAC	Message Authentication Code
MAN	Metropolitan Area Network
MPU	Main Processing Unit
NIST	National Institute of Standards and Technology
OAA	Open Application Architecture
OAP	Open Application Platform
PSU	Power Supply Unit
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RSA	Rivest Shamir and Adleman method for asymmetric encryption
SFP	Small Form-Factor Plugable

Abbreviation	Full spelling
SFP+	Enhanced Small Form-Factor Pluggable
SHA	Secure Hash Algorithm
SRPU	Switching and routing processor unit
SSL	Secure Sockets Layer
XFP	10 Gigabit Small Form-Factor Pluggable

1 Introduction

This document is a non-proprietary Cryptographic Module Security Policy for HPE FlexNetwork MSR1000, MSR2000, MSR3000 and MSR4000 Router Series. The policy describes how the HPE FlexNetwork MSR1000, MSR2000, MSR3000 and MSR4000 Router Series meet the requirements of FIPS 140-2. This document also describes how to configure the HPE FlexNetwork MSR1000, MSR2000, MSR3000 and MSR4000 Router Series in FIPS 140-2 mode. This document was prepared as part of the FIPS 140-2 Security Level 2 validation.

FIPS 140-2 standard details the U.S. Government requirements for cryptographic security appliances. More information about the standard and validation program is available on the NIST website at csrc.nist.gov/groups/STM/cmvp/.

This document includes the following sections:

- Overview
- Security Appliance Validation Level
- Physical Characteristics and Security Appliance Interfaces
- Roles, Services and Authentication
- Services, Key / CSP and Algorithm Tables
- Self-Tests
- Delivery and Operation
- Physical Security Mechanism
- Mitigation of Other Attacks
- Obtaining Documentation and Technical Assistance

NOTE: The following names are referencing the same thing: HPE FlexFabric, HPE Networking devices and HPE Networking Routers.

2 Overview

The HPE FlexNetwork MSR1000, MSR2000, MSR3000 and MSR4000 Router Series are suitable for a range of uses: at the edge of a network, connecting server clusters in a data center, in an enterprise LAN core, and in large-scale industrial networks and campus networks. Each device is based on the HPE Comware Software, Version

7.1.045 platform.

The HPE FlexNetwork MSR1000, MSR2000, MSR3000 and MSR4000 Router Series modules are being validated as a multi-chip standalone module at FIPS 140-2 Security Level 2.

2.1 **HPE FlexNetwork Router Block Level Diagram**

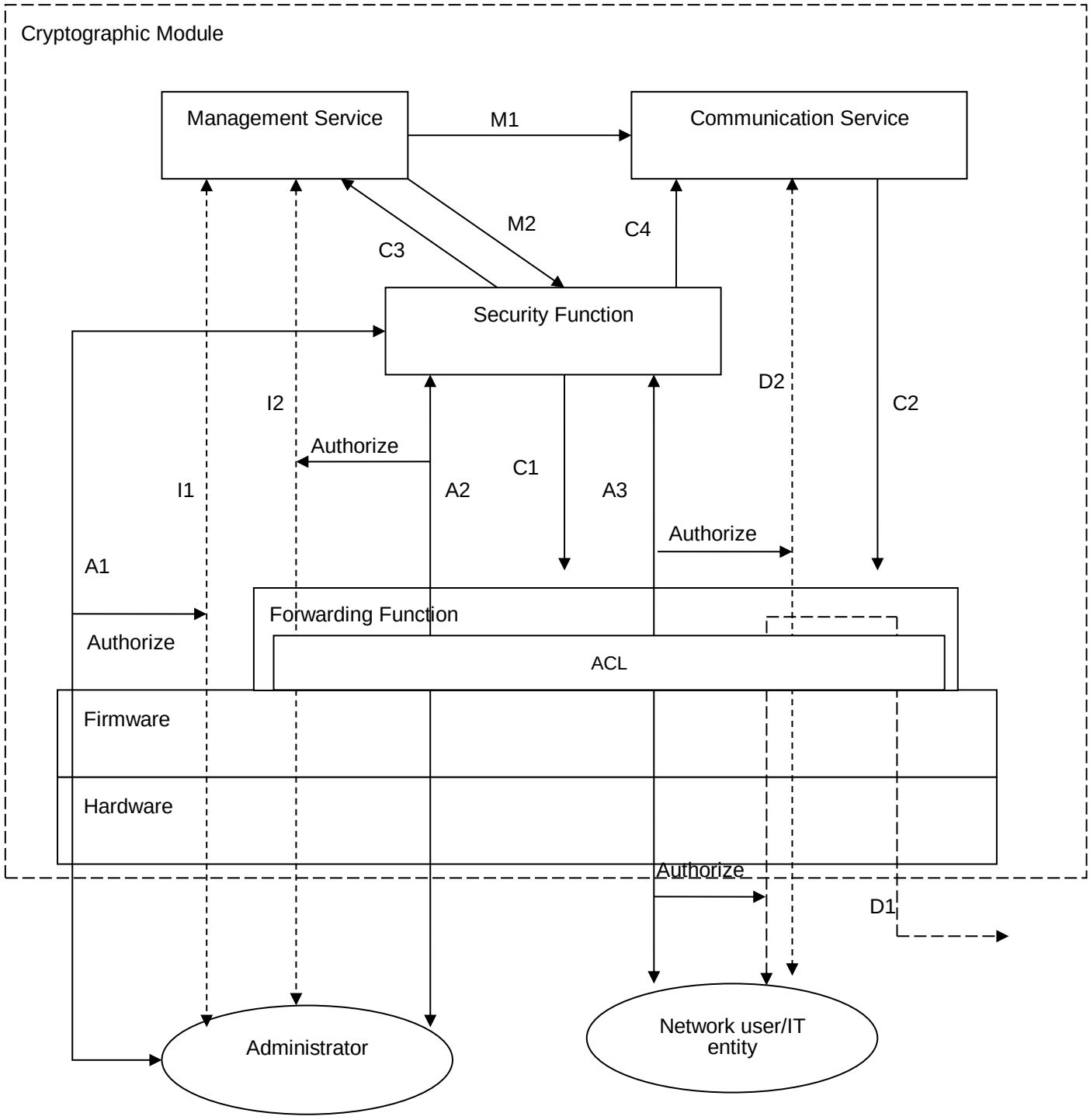


Figure 1 Security Architecture Block Diagram

The cryptographic module provides the following services externally:

1. Management: supports various login methods and configuration interfaces for managing the system.
2. Communication: supports interoperation between the communication protocols at different layers in the protocol stack, such as 802.3, PPP, and IP, and uses the forwarding function to receive/send packets for the local device and forward packets for other devices.

To ensure security, the security function provides appropriate access control for the cryptographic module to identify and authenticate the external entities attempting to access them, and authorize the external entities that pass the identification and authentication. The access control function also records the external entities' accesses to the services, such as the beginning time and end time of a visit. The figure above shows how administrators (crypto officer, user role) and network users access to a cryptographic module service.

M2: The administrator accesses the management service to configure the security function.

M1: The administrator accesses the management service to configure the communication service.

C1: The security function issues the forwarding control ACL or other control measures to the forwarding function for security processing like packet filtering.

D2: The communication service uses the forwarding function to receive and send packets for the local device.

C2: The communication service issues routing entries or MAC address entries to the forwarding function for forwarding packets for other devices.

A1: The administrator connects to a physical management interface (the console for example) of the cryptographic module to access the system management access control service of the security function. If the access succeeds, the I1 access to the management service is authorized. The security function uses the C3 authorization action to authorize the administrator administrative roles.

I1: The administrator accesses the management service through the physical management interface.

A2: The administrator connects to a network interface (such as an Ethernet interface) of the cryptographic module to access the system management access control service of the security function. If the access succeeds, the I2 access to the management service is authorized.

I2: The administrator accesses the management service through the network interface.

A3: A network user connects to a network interface of the cryptographic module to access the communication access control service of the security function. If the access succeeds, D1/D2 are authorized. The security function uses the C4 authorization action to authorize the network user the communication service access privilege, namely, the network access privilege.

D1: Forwarding packets for the network user.

To facilitate cryptographic module management, the administrator is allowed to access the system management service by remote login through a network interface. To prevent the authentication data of the administrator (such as the username and password) from being intercepted and prevent the operation commands from being tampered, the cryptographic module provides the SSH2/HTTPS for secure remote management.

For the management service, the cryptographic module defines predefined roles and custom user roles, which service differs as result of different access permissions.

Each user can switch to a different user role without reconnecting to the device. To switch to a different user role, a user must provide the role switching authentication information. The

authentication is identity-based. All users can be authenticated locally, and optionally supports authentication via a RADIUS and TACACS+ server.

If needed, IPSec can be configured to protect the network data.

No external programs can take control of the cryptographic module, because the cryptographic module does not provide the general-purpose computing service. This ensures the absolute control of the cryptographic module.

2.2 **HPE FlexNetwork MSR1000 Router Series**

2.2.1 **Product overview**

The HPE FlexNetwork MSR1000 Router Series, the next generation of router from HPE, is a component of the HPE FlexBranch solution, which is a part of the comprehensive HPE FlexNetwork architecture. These routers feature a modular design that delivers unmatched application services for small- to medium-sized branch offices. This gives your IT personnel the benefit of reduced complexity, and simplified configuration, deployment, and management.

The MSR1000 series provides an agile, flexible network infrastructure that enables you to quickly adapt to your changing business requirements while delivering integrated concurrent services on a single, easy-to-manage platform.

- Up to 300KMpps forwarding; converged high-performance routing, switching, security, voice, mobility
- Embedded security features with hardware-based encryption, firewall, NAT, and VPNs
- Industry-leading breadth of LAN and WAN connectivity options
- No additional licensing complexity; no cost for advanced features
- Zero-touch solution, with single pane-of-glass management

2.2.2 **Test Modules**

Testing included two models in the HPE FlexNetwork MSR1000 Router Series

- HPE FlexNetwork MSR1002-4 Router (JG875A)
- HPE FlexNetwork MSR1003-8S AC Router (JH060A)

Figure 2 HPE FlexNetwork MSR1002-4 Router (JG875A)

Figure 3 HPE FlexNetwork MSR1003-8S AC Router (JH060A)

Table 1 through Table 3 lists the test configurations for the HPE FlexNetwork MSR1000 Router Series.

Chassis	Controller	Modules
1002-4	HPE FlexNetwork MSR1002-4 AC Router (JG875A)	HPE FlexNetwork A-MSR 9-port 10/100Base-T Switch DSIC Module(JD574B)
		HPE FlexNetwork A-MSR 1-port FXO SIC Module(JD559A)
		HPE FlexNetwork A-MSR 4-port 10/100Base-T Switch SIC Module(JD573B)

Table 1 HPE FlexNetwork MSR1002-4 Router Test configuration 1

Chassis	Controller	Modules
1002-4	HPE FlexNetwork MSR1002-4 AC Router (JG875A)	HPE FlexNetwork A-MSR 1-port FXO SIC Module(JD559A)
		HPE FlexNetwork A-MSR 4-port 10/100Base-T Switch SIC Module(JD573B)

Table 2 HPE FlexNetwork MSR1002-4 Router Test configuration 2

Chassis	Controller	Modules
1003-8S	HPE FlexNetwork MSR1003-8S AC Router (JH060A)	HPE FlexNetwork A-MSR 1-port FXO SIC Module(JD559A)
		HPE FlexNetwork A-MSR 2-port FXS SIC Module(JD560A)
		HPE FlexNetwork A-MSR 1-port T1 Voice SIC Module (JD576A)

Table 3 HPE FlexNetwork MSR1003-8S AC Router Test configuration 1

2.2.3 **Opacity shield and tamper evidence label**

The following figures show the MSR1000 Router Series with opacity shield and tamper evidence label.

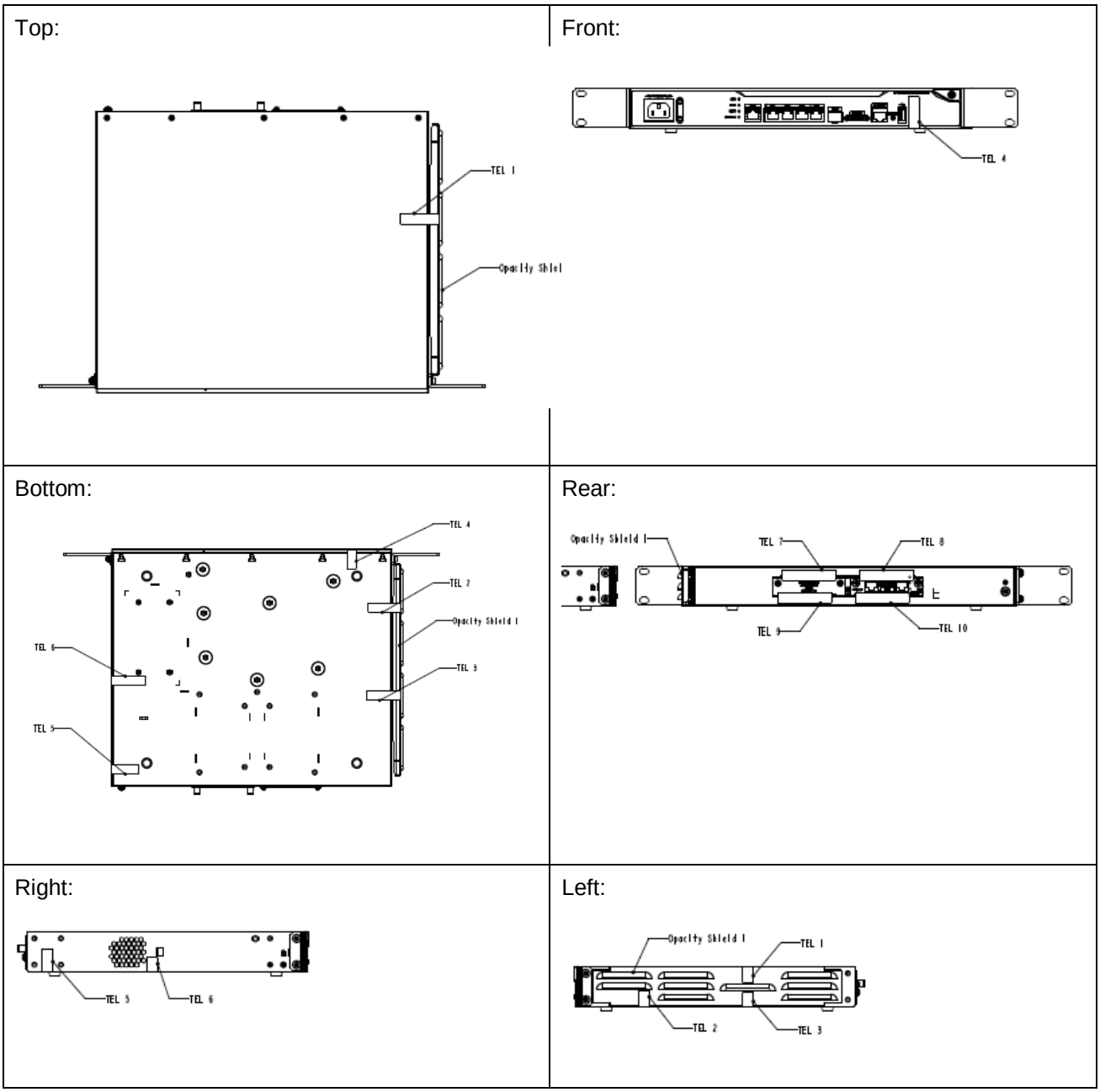


Figure 4 HPE FlexNetwork MSR1002-4 Series Opacity shield and 10 tamper evidence labels

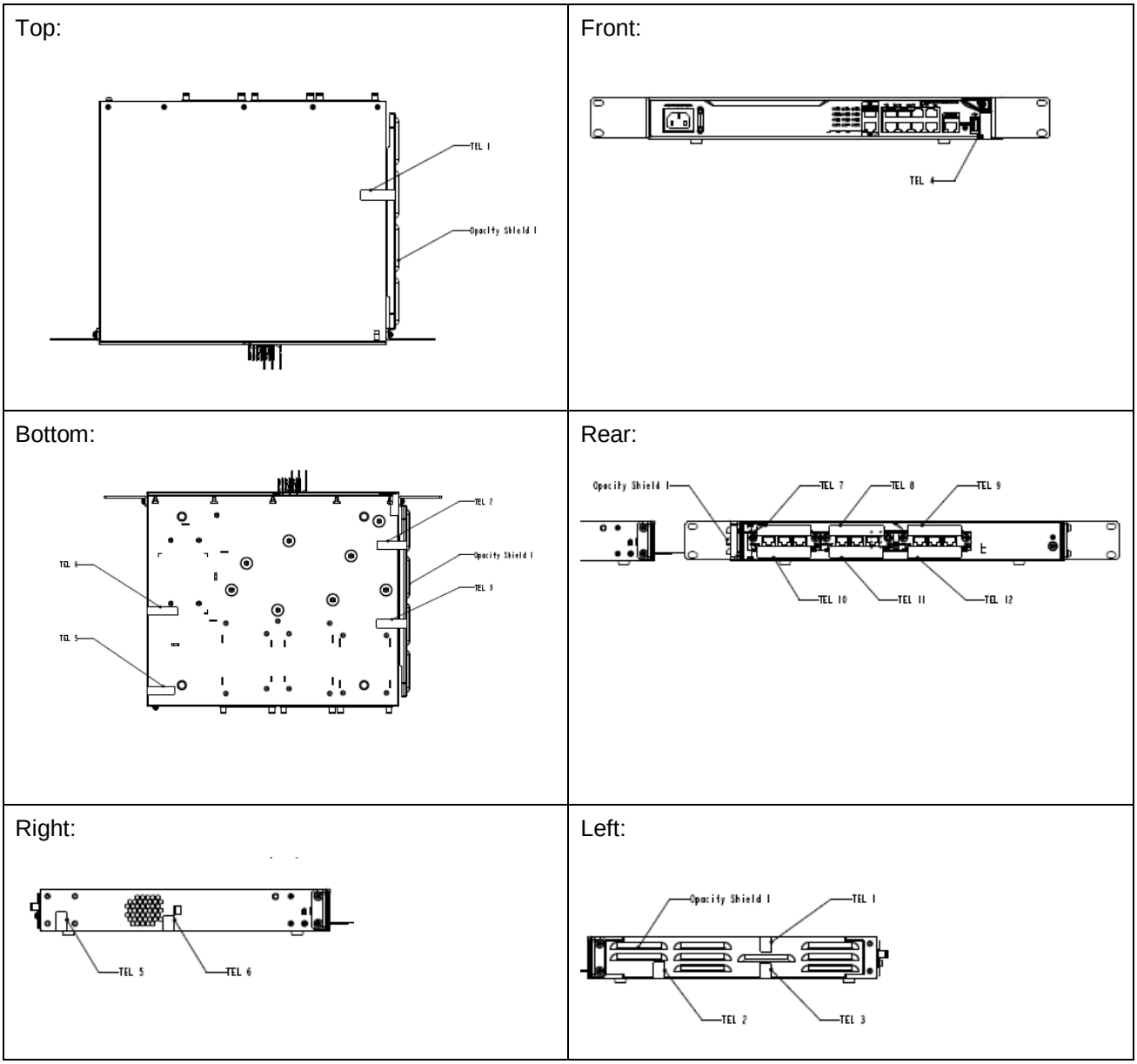


Figure 5 HPE FlexNetwork MSR1003-8S Series Opacity shield and 12 tamper evidence labels

2.3 HPE FlexNetwork MSR2000 Router Series

2.3.1 Product overview

The HPE FlexNetwork MSR2000 Router Series, the next generation of router from HPE, is a component of the HPE FlexBranch solution, which is a part of the comprehensive HPE FlexNetwork architecture. These routers feature a modular design that delivers unmatched application services for small- to medium-sized branch offices. This gives your IT personnel the benefit of reduced complexity, and simplified configuration, deployment, and management.

The MSR2000 series provides an agile, flexible network infrastructure that enables you to quickly adapt to your changing business requirements while delivering integrated concurrent services on a single, easy-to-manage platform.

- Up to 1 Mpps forwarding; converged high-performance routing, switching, security, voice, mobility
- Embedded security features with hardware-based encryption, NAT, and VPNs
- Industry-leading breadth of LAN and WAN connectivity options
- No additional licensing complexity; no cost for advanced features
- Zero-touch solution, with single pane-of-glass management

2.3.2 **Test Modules**

Testing included four models in the HPE FlexNetwork MSR2000 Router Series

- HPE FlexNetwork MSR2003 AC Router (JG411A)
- HPE FlexNetwork MSR2003 TAA-compliant AC Router (JG866A)
- HPE FlexNetwork MSR2004-24 AC Router (JG734A)
- HPE FlexNetwork MSR2004-48 Router (JG735A)

Figure 6 HPE FlexNetwork MSR2003 AC Router (JG411A) and HPE FlexNetwork MSR2003 TAA-compliant AC Router (JG866A)

Figure 7 HPE FlexNetwork MSR2004-24 AC Router (JG734A)

Figure 8 HPE FlexNetwork MSR2004-48 Router (JG735A)

Table 4 through Table 7 lists the test configurations for the HPE FlexNetwork MSR2000 Router Series.

Chassis	Controller	Modules
MSR2003	MSR2003 AC Router(JG411A) & (JG866A)	HPE FlexNetwork A-MSR 2-port FXO SIC Module(JD558A)
		HPE FlexNetwork A-MSR 9-port 10/100Base-T Switch DSIC Module (JD574B)

Table 4 HPE FlexNetwork MSR2003 AC Router Test configuration 1

Chassis	Controller	Modules
MSR2003	MSR2003 AC Router(JG411A) & (JG866A)	HPE FlexNetwork A-MSR 1-port FXO SIC Module(JD559A)
		HPE FlexNetwork A-MSR 1-port T1 Voice SIC Module(JD576A)
		HPE FlexNetwork A-MSR 2-port ISDN-S/T Voice SIC Module(JF821A)

Table 5 HPE FlexNetwork MSR2003 AC Router Test configuration 2

Chassis	Controller	Modules
MSR2004-24	HPE FlexNetwork MSR2004-24 AC Router(JG734A)	HPE FlexNetwork A-MSR 2-port FXS SIC Module(JD560A)
		HPE FlexNetwork A-MSR 1-port FXO SIC Module(JD559A)
		HPE FlexNetwork A-MSR 2-port ISDN-S/T Voice SIC Module (JF821A)
		HPE FlexNetwork A-MSR 1-port T1 Voice SIC Module(JD576A)

Table 6 HPE FlexNetwork MSR2004-24 AC Router Test configuration 1

Chassis	Controller	Modules
MSR2004-48	HPE FlexNetwork MSR2004-48 Router(JG735A)	HPE FlexNetwork A-MSR 1-port FXO SIC Module(JD559A)
		HPE FlexNetwork A-MSR 1-port T1 Voice SIC Module(JD576A)
		HPE FlexNetwork A-MSR 2-port FXS SIC Module(JD560A)
		HPE FlexNetwork A-MSR 2-port ISDN-S/T Voice SIC Module(JF821A)

Table 7 HPE FlexNetwork MSR2004-48 Router Test configuration 1

2.3.3 **Opacity shield and tamper evidence label**

The following figures show the MSR2000 Router Series with opacity shield and tamper evidence label.

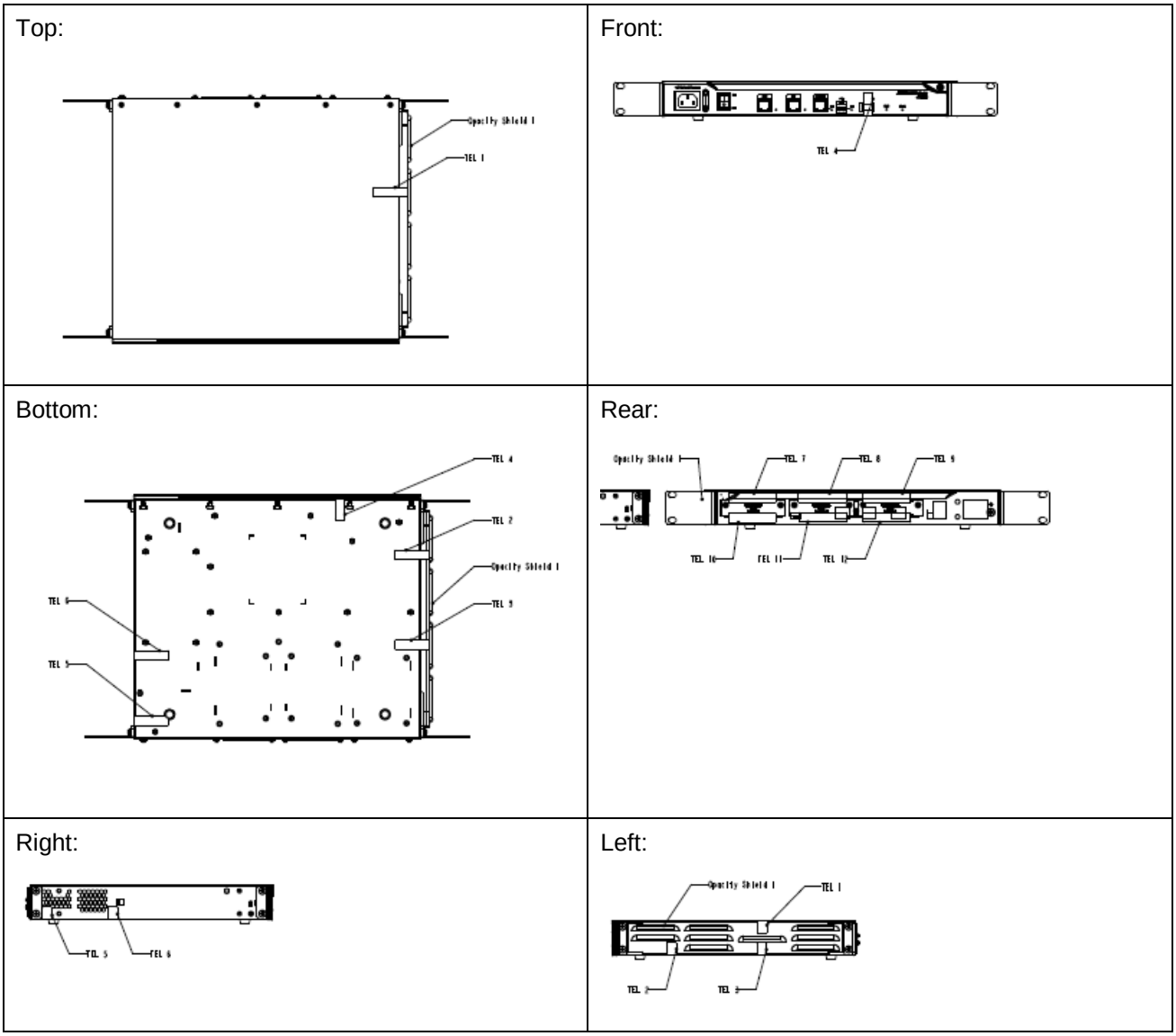


Figure 9 HPE FlexNetwork MSR2003 AC Router (JG411A) and HPE FlexNetwork MSR2003 TAA-compliant AC Router (JG866A) Opacity shield and 12 tamper evidence labels

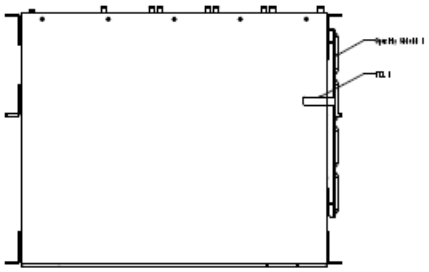
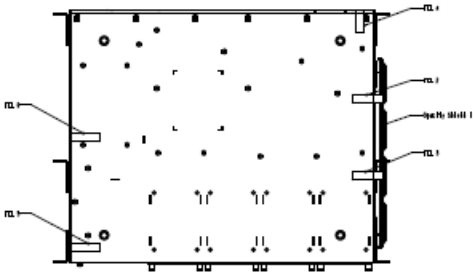
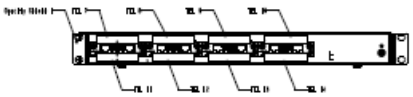
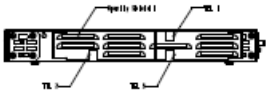
Top: 	Front: 
Bottom: 	Rear: 
Right: 	Left: 

Figure 10 HPE FlexNetwork MSR2004-24 AC Router (JG734A) Opacity shield and 14 tamper evidence labels

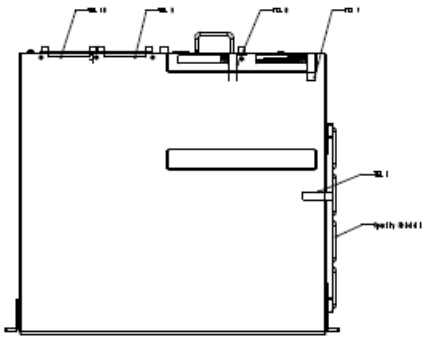
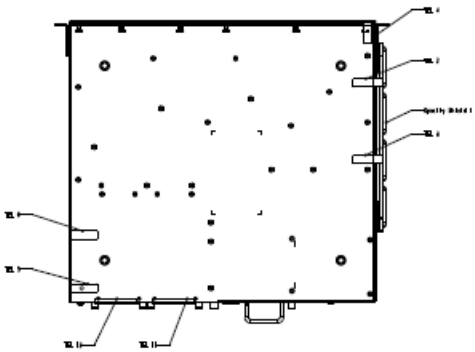
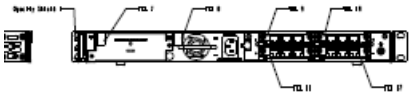
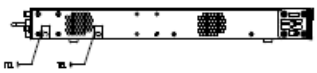
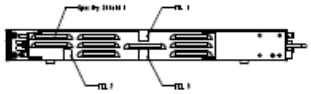
Top: 	Front: 
Bottom: 	Rear: 
Right: 	Left: 

Figure 11 HPE FlexNetwork MSR2004-48 Router (JG735A) Opacity shield and 12 tamper evidence labels

2.4 **HPE FlexNetwork MSR3000 Router Series**

2.4.1 **Product overview**

The HPE FlexNetwork MSR3000 Router Series, the next generation of router from HPE, is a component of the HPE FlexBranch solution, which is a part of the comprehensive HPE FlexNetwork architecture. These routers feature a modular design that delivers unmatched application services for medium- to large-sized branch offices. This gives your IT personnel the benefit of reduced complexity, and simplified configuration, deployment, and management.

The MSR3000 routers use the latest multicore CPUs, offer Gigabit switching, provide an enhanced PCI bus, and ship with the latest version of HPE Comware software to help ensure high performance with concurrent services. The MSR3000 series provides a full-featured, resilient routing platform, including IPv6 and MPLS, with up to 5 Mpps forwarding capacity and 3.3 Gb/s of IPSec VPN encrypted throughput. These routers also support HPE Open Application Platform (OAP) modules to deliver integrated industry-leading HPE AllianceOne partner applications such as virtualization, unified communications and collaboration (UC&C), and application optimization capabilities.

The MSR3000 series provides an agile, flexible network infrastructure that enables you to quickly adapt to changing business requirements while delivering integrated concurrent services on a single, easy-to-manage platform

- Up to 5 Mpps forwarding performance; support for multiple concurrent services
- Open Application Platform for HPE AllianceOne applications like WAN acceleration and Microsoft® Lync
- Embedded security features with hardware-based encryption, firewall, NAT, and VPNs
- No additional licensing complexity; no cost for advanced features
- Zero-touch solution, with single pane-of-glass management

2.4.2 **Test Modules**

Testing included three models in the HPE FlexNetwork MSR3000 AC Router Series

- HPE FlexNetwork MSR3012 AC Router (JG409A)
- HPE FlexNetwork MSR3044 Router (JG405A)
- HPE FlexNetwork MSR3064 Router (JG404A)

Figure 12 HPE FlexNetwork MSR3012 AC Router (JG409A)

Figure 13 HPE FlexNetwork MSR3044 Router (JG405A)

Figure 14 HPE FlexNetwork MSR3064 Router (JG404A)

Table 8 through Table 10 lists the test configurations for the HPE FlexNetwork MSR3000 Router Series.

Chassis	Controller	Modules
MSR3012	HPE FlexNetwork MSR3012 AC Router(JG409A)	HPE FlexNetwork MSR 1p E1/CE1/PRI SIC Mod(JG604A)
		HPE FlexNetwork A-MSR 8-port Async Serial SIC Module(JF281A)
		HPE FlexNetwork MSR 1p T1 Voice HMIM Mod(JG430A)

Table 8 HPE FlexNetwork MSR3012 AC Router Test configuration 1

Chassis	Controller	Modules
MSR3044	HPE FlexNetwork MSR3044 Router(JG405A)	HPE FlexNetwork A-MSR 1-port FXO SIC Module(JD559A)
		HPE FlexNetwork A-MSR 2-port FXS SIC Module(JD560A)
		HPE FlexNetwork A-MSR 1-port FXS SIC Module(JD561A)
		HPE FlexNetwork MSR 4-port Enhanced Sync / Async Serial HMIM Module(JG442A)
		HPE FlexNetwork MSR 1-port OC-3c / STM-1c POS HMIM Module(JG438A)
		HPE FlexNetwork MSR 8-port Enhanced Sync / Async Serial HMIM Module(JG443A)
		HPE FlexNetwork MSR 4p FXO HMIM Mod(JG447A)

Table 9 HPE FlexNetwork MSR3044 Router Test configuration 1

Chassis	Controller	Modules
MSR3064	HPE FlexNetwork MSR3064 Router(JG404A)	HPE FlexNetwork MSR 1p E1/CE1/PRI SIC Mod(JG604A)
		HPE FlexNetwork A-MSR 8-port Async Serial SIC Module(JF281A)
		HPE FlexNetwork A-MSR 802.11b/g/n SIC Module (NA)(JG211A)
		HPE FlexNetwork MSR 4p Enh Sync/Async Srl SIC MOD(JG737A)
		HPE FlexNetwork MSR 1p T1 Voice HMIM Mod (Ports 5&7)(JG430A)
		HPE FlexNetwork MSR 4p FXO HMIM Mod(JG447A)
		HPE FlexNetwork MSR 0.5U HMIM Adapter Module(JG415A) HPE FlexNetwork MSR 1-port OC-3 ATM MIM Module(JD624A)
		HPE FlexNetwork MSR 0.5U HMIM Adapter Module(JG415A) HPE FlexNetwork MSR 2-port 10/100 MIM Module(JD613A)
		HPE FlexNetwork MSR 4p T1/Fractional T1 HMIM Mod(JG457A)
		HPE FlexNetwork MSR 0.5U HMIM Adapter Module(JG415A) HPE FlexNetwork MSR 1p T3/CT3/FT3 HMIM Mod(JG435A)

Table 10 HPE FlexNetwork MSR3064 Router Test configuration 1

2.4.3 **Opacity shield and tamper evidence label**

The following figures show the MSR3000 Router Series with opacity shield and tamper evidence label.

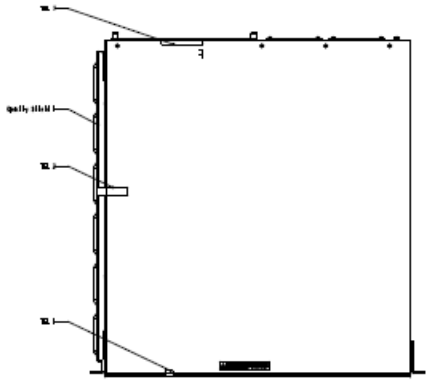
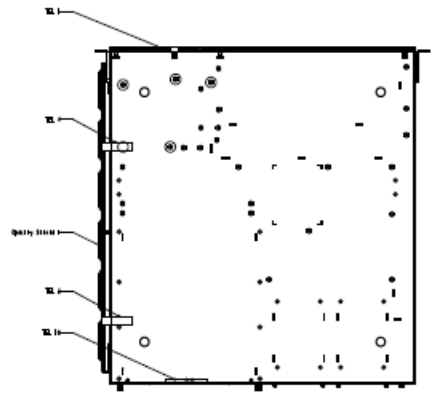
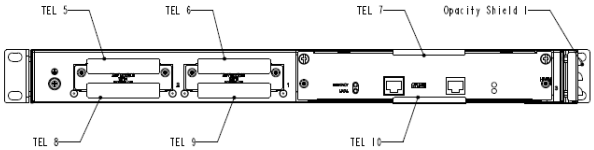
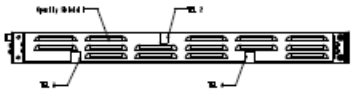
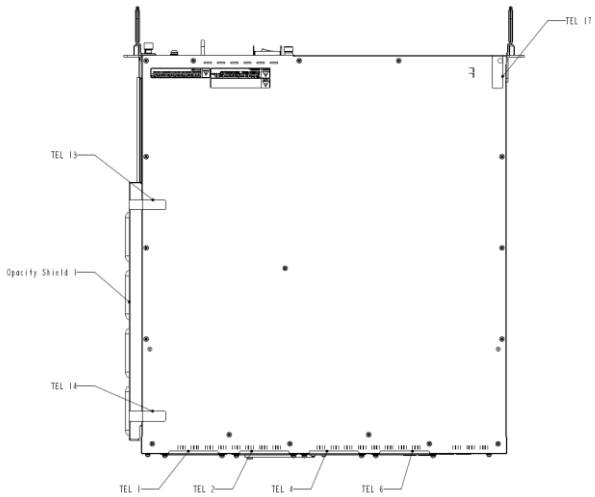
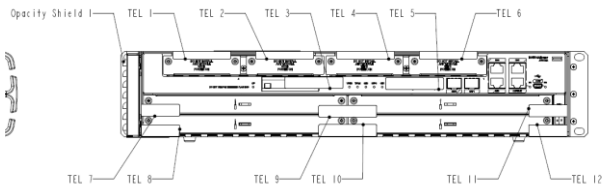
<table>
<tr><td>Top:
  </td><td>Front:
 
</td></tr>
<tr><td>Bottom:
  </td><td>Rear:
 
</td></tr>
<tr><td>Right:
  </td><td>Left:
  </td></tr>
</table>

Figure 15 HPE FlexNetwork MSR3012 AC Router (JG409A) Opacity shield and 10 tamper evidence labels

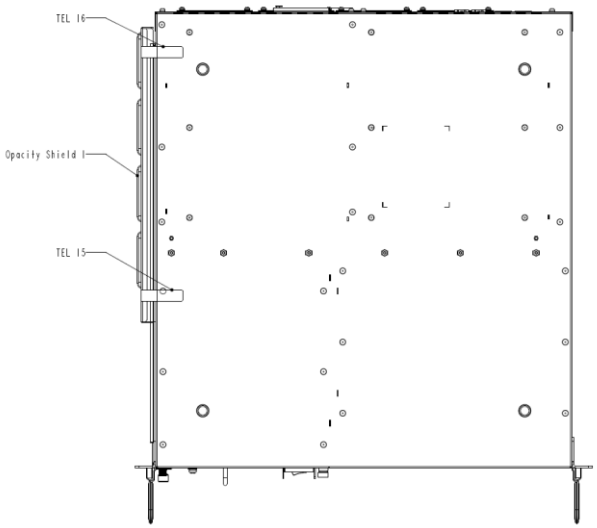
Top:



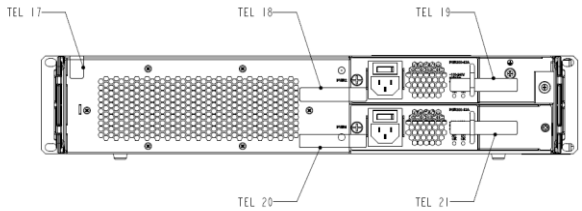
Front:



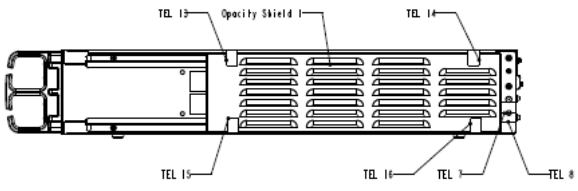
Bottom:



Rear:



Right:



Left:

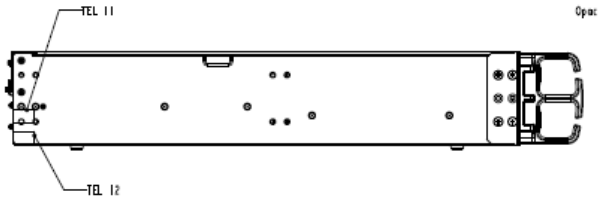
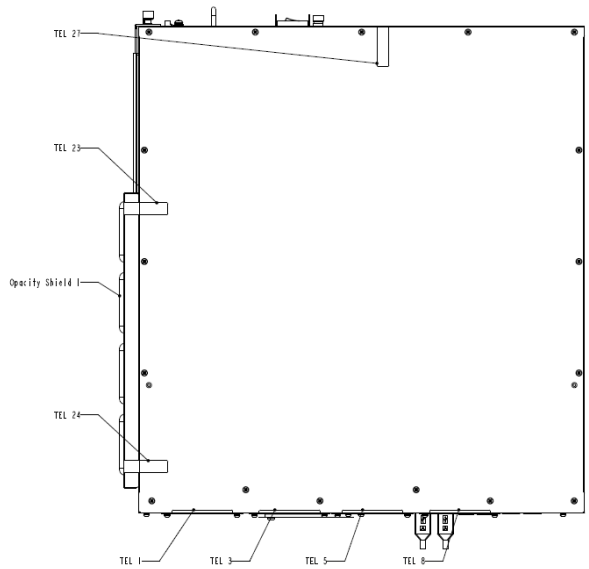
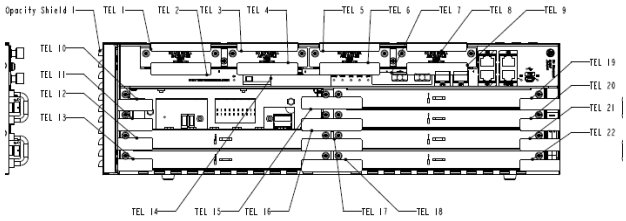


Figure 16 HPE FlexNetwork MSR3044 Router (JG405A) Opacity shield and 21 tamper evidence labels

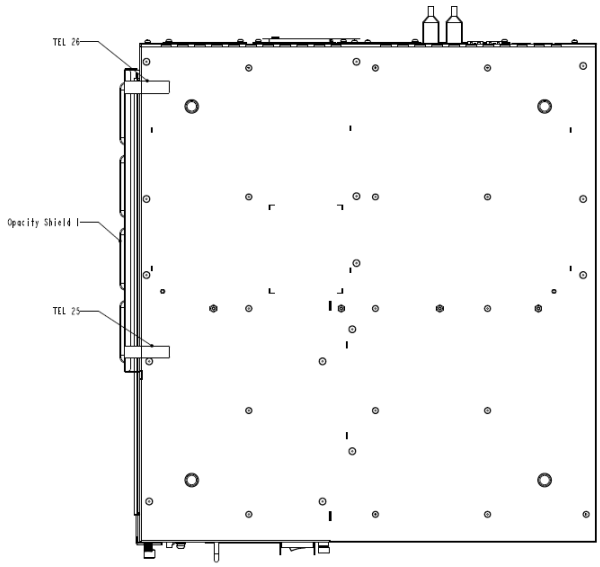
Top:



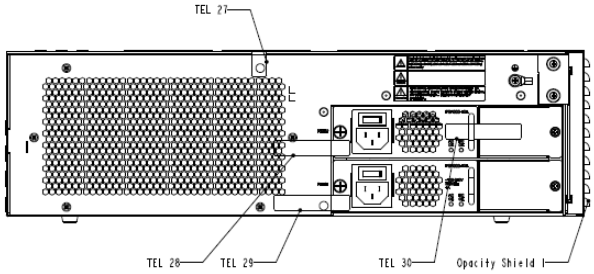
Front:



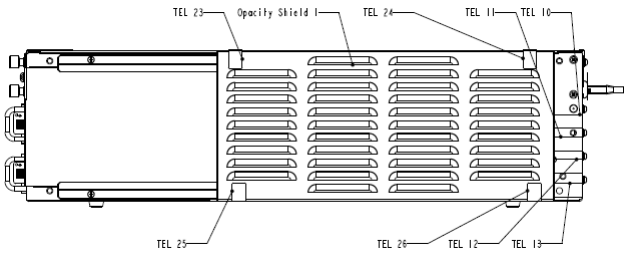
Bottom:



Rear:



Right:



Left:

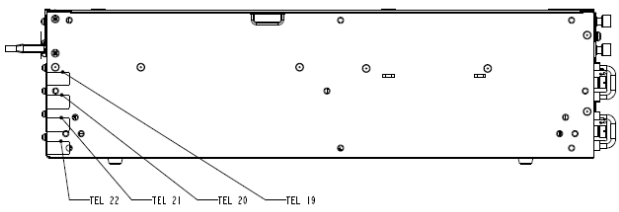


Figure 17 HPE FlexNetwork MSR3064 Router (JG404A) Opacity shield and 30 tamper evidence labels

2.5 **HPE FlexNetwork MSR4000 Router Series**

2.5.1 **Product overview**

The HPE FlexNetwork MSR4000 Router Series, the next generation of router from HPE is a component of the HPE FlexBranch solution, which is a part of the comprehensive HPE FlexNetwork architecture. These routers feature a modular design that delivers unmatched application services for extra-large branch offices, headquarters, and campuses. This gives your IT personnel the benefit of reduced complexity, and simplified configuration, deployment, and management. The MSR4000 series leverages separated data and control planes, dual main processing units (MPUs), and support for up to four power supplies, which provides outstanding performance and reliability.

The MSR4000 routers provide a full-featured, resilient routing platform with the latest multicore CPUs, offer 10 Gigabit SFP+ integrated, provide an enhanced PCI bus, and ship with the latest version of HPE Comware software to help ensure high performance with concurrent services. The MSR4000 series provides a full-featured, resilient routing platform, including IPv6 and MPLS, with up to 36 Mpps forwarding capacity and 28 Gb/s of IPSec VPN encrypted throughput. These routers also support HPE Open Application Platform (OAP) modules to deliver integrated industry-leading HPE AllianceOne partner applications such as virtualization, unified communications and collaboration (UC&C), and application optimization capabilities.

The MSR4000 series provides an agile, flexible network infrastructure that enables you to quickly adapt to your changing business requirements while delivering integrated concurrent services on a single, easy-to-manage platform。

- Up to 36 Mpps forwarding performance; support for multiple concurrent services
- High reliability with separated hardware data and control planes, and dual MPUs
- Open Application Platform for HPE AllianceOne applications
- Powerful aggregation capacity; integrated 10GbE; support for up to 64 E1 or eight E3/T3 ports
- Zero-touch solution with single pane-of-glass management

2.5.2 **Test Modules**

Testing included two models in the HPE FlexNetwork MSR4000 Router Series

- HPE FlexNetwork MSR4060 Router Chassis (JG403A)
- HPE FlexNetwork MSR4080 Router Chassis (JG402A)

Figure 18 HPE FlexNetwork MSR4060 Router Chassis (JG403A)

Figure 19 HPE FlexNetwork MSR4080 Router Chassis (JG402A)

Table 11 through Table 12 lists the test configurations for the HPE FlexNetwork MSR4000 Router Series.

Chassis	Controller	Modules
MSR4060	HPE FlexNetwork MSR4000 TAA-compliant MPU-100 Main Processing Unit (JG869A)	HPE FlexNetwork MSR 0.5U HMIM Adapter Module(JG415A) HPE FlexNetwork MSR 1p T3/CT3/FT3 HMIM Mod(JG435A)
		HPE FlexNetwork MSR 0.5U HMIM Adapter Module(JG415A) HPE FlexNetwork MSR 4p T1/Fractional T1 HMIM Mod(JF254B)
		HPE FlexNetwork MSR 4p FXO HMIM Mod(JG447A)

Table 11 HPE FlexNetwork MSR4060 Router Chassis Test configuration 1

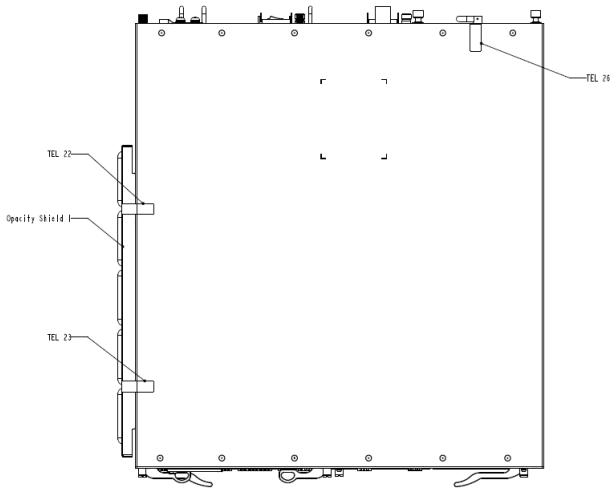
Chassis	Controller	Modules
MSR4080	HPE FlexNetwork MSR4000 TAA-compliant MPU-100 Main Processing Unit (JG869A)	HPE FlexNetwork MSR 16-port Async Serial Interface MIM Module(JF841A)
		HPE FlexNetwork MSR 1U HMIM Adapter Module(JG416A) HPE FlexNetwork MSR 16-port Async Serial Interface MIM Module(JF841A)
		HPE FlexNetwork MSR 0.5U HMIM Adapter Module(JG415A) HPE FlexNetwork MSR 4p T1/Fractional T1 HMIM Mod(JF254B)
		HPE FlexNetwork MSR 0.5U HMIM Adapter Module(JG415A) HPE FlexNetwork 6600 8-port T1 MIM Router Module(JC160A)
		HPE FlexNetwork MSR 0.5U HMIM Adapter Module(JG415A) HPE FlexNetwork 6600 8-port Fractional T1 MIM Router Module(JC159A)
		HPE FlexNetwork MSR 0.5U HMIM Adapter Module(JG415A) HPE FlexNetwork 4-port ISDN BRI S/T Voice Interface MIM Module(JF837A)

Table 12 HPE FlexNetwork MSR4080 Router Chassis Test configuration 1

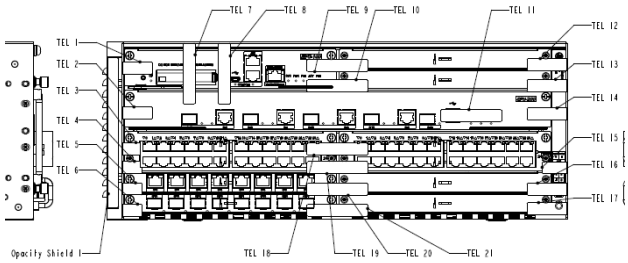
2.5.3 **Opacity shield and tamper evidence label**

The following figures show the MSR4000 Router Series with opacity shield and tamper evidence label.

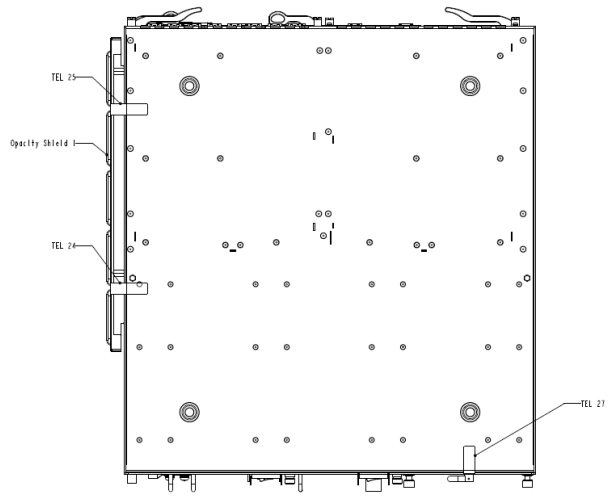
Top:



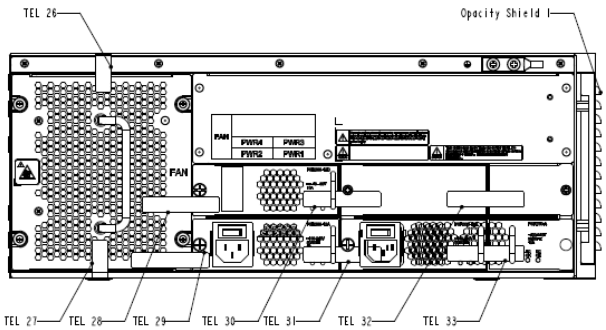
Front:



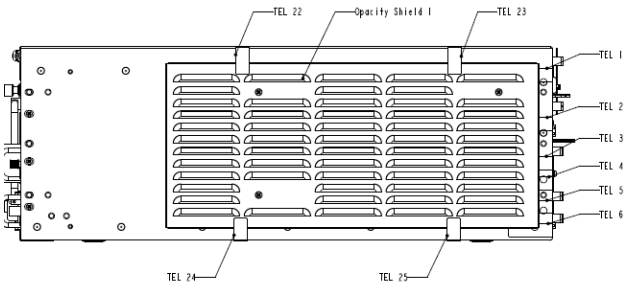
Bottom:



Rear:



Right:



Left:

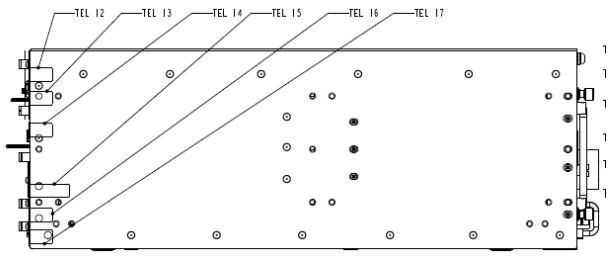


Figure 20 HPE FlexNetwork MSR4060 Router Chassis (JG403A) Opacity shield and 33 tamper evidence labels

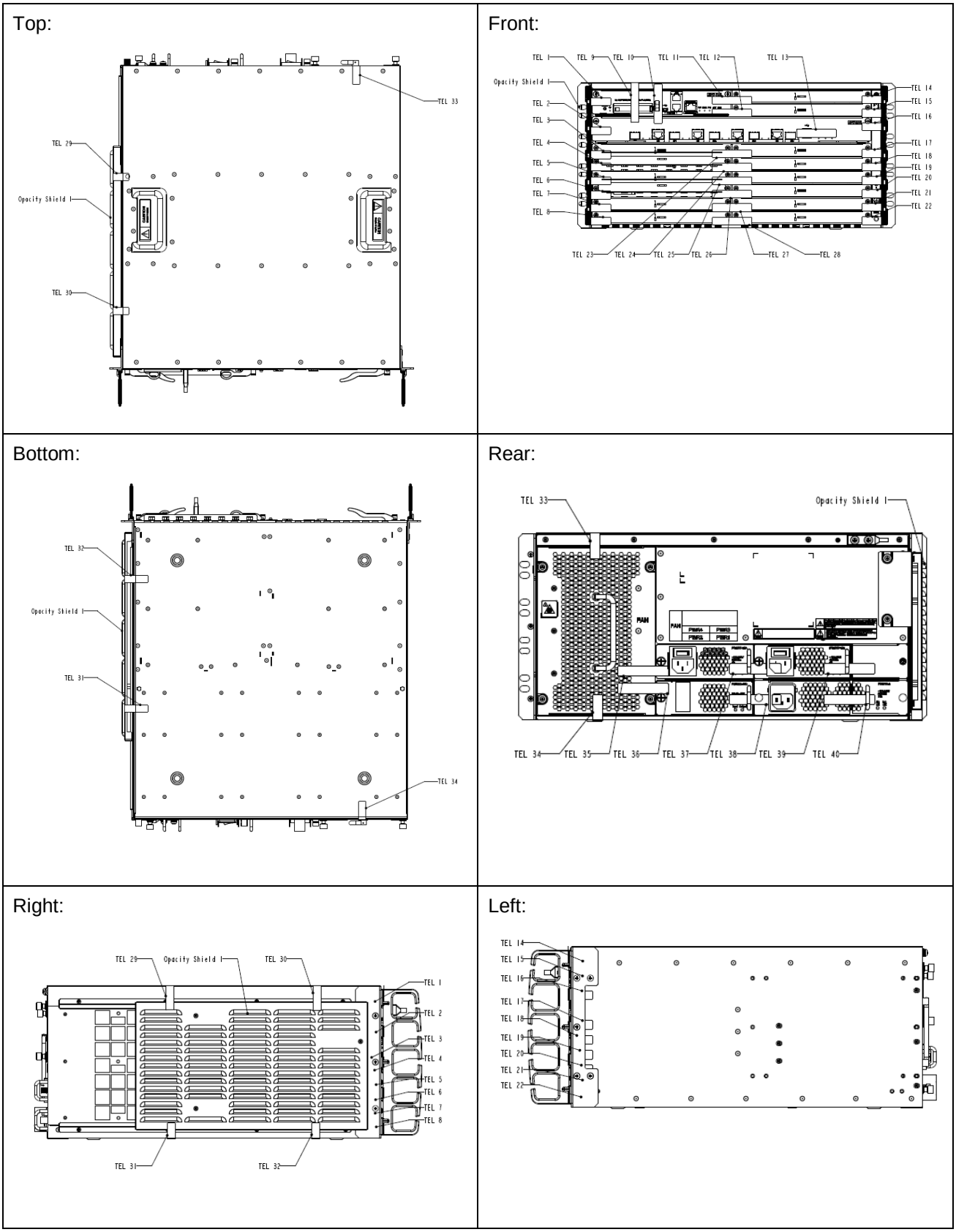


Figure 21 HPE FlexNetwork MSR4080 Router Chassis (JG402A) Opacity shield and 40 tamper evidence labels

3 Security Appliance Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2.

Table 13 Validation Level by Section

No.	Area	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	3
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key management	2
8	Electromagnetic Interface/Electromagnetic Compatibility	2
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
12	Overall Level	2

4 Physical Characteristics and Security Appliance Interfaces

Each router in the HPE FlexNetwork MSR1000, MSR2000, MSR3000 and MSR4000 Router Series is a multi-chip standalone security appliance, and the cryptographic boundary is defined as encompassing the “top,” “front,” “rear,” “left,” “right,” and “bottom” surfaces of the case. The general components of the HPE FlexNetwork MSR1000, MSR2000, MSR3000 and MSR4000 Router Series include firmware and hardware, which are placed in the three-dimensional space within the case. The internal components of the SIC/DSIC/MIM/HMIM modular cards listed in test configurations in sections 2.2.2, 2.3.2, 2.4.2, and 2.5.2 of this document are excluded from FIPS 140-2 requirements.

4.1 HPE FlexNetwork MSR1000 Router Series

The HPE FlexNetwork MSR1000 router series provides:

Item	MSR1002-4	MSR1003-8S
Console/AUX port	1	
USB console port	1	
Gigabit Ethernet port	5	10
Gigabit Ethernet Fiber port	1	0
Serial Port	1	0
Memory	512MB DDR3	
Flash	256MB	
SIC/DSIC slot	(2) SIC slots or (1) DSIC slot	(3) SIC slots or (1) DSIC slot and (1) SIC slot
Dimensions (H × W × D) (excluding rubber feet and mounting brackets)	360mm×300mm×44.2mm	
AC power supply	Rated voltage range: 100 VAC to 240 VAC @ 50 Hz/60 Hz	
Rated power for AC power supply	54 W	
Operating temperature	0°C to 45°C (32°F to 113°F)	
Relative humidity (noncondensing)	5% to 90%	

The documents in HP website (https://www.hpe.com/us/en/product-catalog/networking/networking-routers/pip.hpe-flexnetwork-msr1000-router-series.6796027.html) describe the ports in detail along with the interpretation of the LEDs.

4.2 HPE FlexNetwork MSR2000 Router Series

The HPE FlexNetwork MSR2000 router technical specifications:

Item	MSR2003	MSR2004-24	MSR2004-48
Console/AUX port	1		
USB console port	1		
USB port	1		
Gigabit Ethernet port	2	3 + 24 RJ-45 autosensing 10/100/1000 LAN 1 SFP fixed Gigabit Ethernet	3 + 48 RJ-45 autosensing 10/100/1000 LAN
Memory	1 GB DDR3		
Flash	256 MB		
SIC/DSIC slot	3 SIC slots or 1 DSIC slot and 1 SIC slot	4 SIC slots	4 SIC slots
Dimensions (H × W × D) (excluding rubber feet and mounting brackets)	14.17(w) x 11.81(d) x 1.74(h) in (36 x 30 x 4.42 cm) (1U height)	17.32(w) x 14.17(d) x 1.74(h) in (43.99 x 35.99 x 4.42 cm) (1U height)	17.32(w) x 15.75(d) x 1.74(h) in (43.99 x 40.01 x 4.42 cm) (1U height)
AC power supply	Rated voltage range: 100 VAC to 240 VAC @ 50 Hz/60 Hz		
Rated power for AC power supply	54 W	54 W	150 W
Operating temperature	0°C to 45°C (32°F to 113°F)		
Relative humidity (noncondensing)	5% to 90%		

The documents in HP website (https://www.hpe.com/us/en/product-catalog/networking/networking-routers/pip.hpe-flexnetwork-msr2000-router-series.5408894.html) describe the ports in detail along with the interpretation of the LEDs.

4.3 HPE FlexNetwork MSR3000 Router Series

The HPE FlexNetwork MSR3000 router series technical specifications:

Item	MSR3012	MSR3044	MSR3064
CON/AUX ports	1		
USB console ports	1		
USB ports	2		
Gigabit Ethernet ports	3		
SIC/DSIC slots	2 SIC slots	4 SIC slots/2 DSIC slots	
HMIM slots	1	4	6
VPM slots	N/A	2	2
Memory	1 GB DDR3	DDR3 2 GB (default) 4 GB (maximum)	
Built-in CF card memory	256 MB		
External CF card memory	4 GB (maximum)		
CF card slot	1		
Dimensions (H × W × D) (excluding rubber feet and mounting brackets)	44.2 × 440 × 484.3 mm (1.74 × 17.32 × 19.07 in)	88.1 × 440 × 480 mm (3.47 × 17.32 × 18.90 in)	130.5 × 440 × 480 mm (5.14 × 17.32 × 18.90 in)
AC power supply	Rated voltage range: 100 VAC to 240 VAC @ 50 Hz/60 Hz		
DC power supply	Rated voltage range: –48 VDC to –60 VDC		
Rated power for AC/DC power supply	125 W	AC: 300 W	AC: 300 W
Rated power for PoE power supply	Not supported	750 W	750 W
Rated power for each PoE port	15.4 W		
RPS power	800 W	N/A	N/A
Operating temperature	0°C to 45°C (32°F to 113°F)		
Relative humidity (noncondensing)	5% to 90%		

The documents in HP website (https://www.hpe.com/us/en/product-catalog/networking/networking-routers/pip.hpe-flexnetwork-msr3000-router-series.5408895.html) describe the ports in detail along with the interpretation of the LEDs.

4.4 HPE FlexNetwork MSR4000 Router Series

The HPE FlexNetwork MSR4000 router series technical specifications:

Item	MSR4060	MSR4080
MPU slot	2	
SPU slot	1	
HMIM slot	6	8
Dimensions (H × W × D), excluding rubber feet and mounting brackets	175.1 × 440 × 480 mm (6.89 × 17.32 × 18.90 in)	219.5 × 440 × 480 mm (8.64 × 17.32 × 18.90 in)
Operating temperature	0°C to 45°C (32°F to 113°F)	
Operating humidity (noncondensing)	5% to 90%	

MPU-100 specifications:

Item	Specification
Console port	1
AUX port	1
GE management port	1
USB console port	1
USB port	1
Memory	2 GB DDR3 (default) 4 GB DDR3 (maximum)
CF card	512 MB (default) 4 GB (maximum)
CF card slot	1
Flash	8 MB

SPU-100/SPU-200/SPU-300 specifications:

Item	SPU-100	SPU-200	SPU-300
USB port	2		
VPM slot	2		
Combo interface	4		

SFP+ port	0	1	1
Applicable router model	MSR4060/4080		
Applicable MPU	MPU-100		

The documents in HP website (https://www.hpe.com/us/en/product-catalog/networking/networking-routers/pip.hpe-flexnetwork-msr4000-router-series.5408896.html) describe the ports in detail along with the interpretation of the LEDs.

4.5 Physical Interfaces Mapping

The physical interfaces provided by the HPE Networking products map to four FIPS 140-2 defined logical interface: data input, data output, control input and status output. Table 14 presents the mapping.

Table 14 Correspondence between Physical and Logical Interfaces

Physical Interface	FIPS 140-2 Logical Interface
Networking ports	Data Input Interface
Console port	
Management Ethernet port	
CF card slot	
USB ports	
Networking ports	Data Output Interface
Console port	
Management Ethernet port	
CF card slot	
USB ports	
Networking ports	Control Input Interface
Console port	
Management Ethernet port	
Power switches	
Reset Switch	
Port status LED mode switching button	
Networking ports	Status Output Interface
Console port	
Management Ethernet port	
LEDs	
Power Slot	Power Interface
Backplane	

5 Roles, Services, and Authentication

5.1 Roles

The HPE FlexNetwork MSR1000, MSR2000, MSR3000 and MSR4000 Router Series provides 18 predefined roles and 64 custom user roles. There are 16 roles (below) in the device that operators may assume:

- network-admin, level-15, level-9 and security-audit which are the FIPS Crypto-Officer Role,
- network-operator, level 0 ~ level 8, level 10 ~ level 14 and 64 custom user roles which are defined as the FIPS User Role.

Table 15 presents the roles and roles description. The devices allow multiple management users to operate the appliance simultaneously.

The HPE Networking routers do not employ a maintenance interface and do not have a maintenance role.

Table 15 Roles and Role description

FIPS Role	Comware Role Name	Role Description
Crypto-Officer	network-admin	● Accesses all features and resources in the system, except for the **display security-logfile summary**, **info-center security-logfile directory**, and **security-logfile save** commands.
	level-15	Has the same rights as network-admin
	Level-9	Has access to all features and resources except those in the following list. ● RBAC non-debugging commands. ● Local users. ● File management. ● Device management. ● The display history-command all command.
	security-audit	Security log manager. The user role has the following access to security log files: ● Access to the commands for displaying and maintaining security log files (for example, the dir, display security-logfile summary, and more commands). ● Access to the commands for managing security log files and security log file system (for example, the info-center security-logfile directory, mkdir, and security-logfile save commands). Only the security-audit user role has access to security log files.
User	network-operator	● Accesses the display commands for all features and resources in the system, except for commands such as display history-command all and display security-logfile summary. ● Enables local authentication login users to change their own password.
	level-0	Has access to diagnostic commands, including ping, tracert, and ssh2.

	level-1	Has access to the display commands of all features and resources in the system except display history-command all. The level-1 user role also has all access rights of the user role level-0.
	custom user role; level-2 to level-8; level-10 to level-14	Have no access rights by default. Access rights are configurable.

5.2 **Authentication Mechanisms**

HPE networking devices support identity-based authentication, and role-based access control.

- Identity-based authentication

  Each user is authenticated upon initial access to the device. The authentication is identity-based. All users can be authenticated locally, and optionally supports authentication via a RADIUS and TACACS+ server.

  To logon to the appliances, an operator must connect to it through one of the management interfaces (console port, SSH) and provide a password.

  A user must be authenticated using usernames and passwords. The minimum password length is 15 characters, and the maximum is 63. The passwords must contain at least one lower case letter (26), one upper case letter (26), one special character (32) and one numeric character (10). The remaining eleven characters can be a lower case letter (26), an upper case letter (26), a special character (32) and/or a numeric character (10) equaling 94 possibilities per character. Therefore, for a 15 characters password, the probability of randomly guessing the correct sequence is 1 in 3.16228xE^29[1] (this calculation is based on the use of the typical standard American QWERTY computer keyboard).

  In order to guess the password in 1 minute with close to probability 1 requires 3.16228xE^29 trials, which is stronger than the one in a million chance required by FIPS 140-2. By default, the maximum number of consecutive failed login attempts is three and a user failing to log in after the specified number of attempts must wait for one minute before trying again. Using Anderson's formula to calculate the probability of guessing a password in 1 minute:

  - *P* probability of guessing a password in specified period of time
  - *G* number of guesses tested in 1 time unit
  - *T* number of time units

[1] Calculation is: 94^15 (total combinations of alpha, numeric, and special characters) - 68^15 (combinations with no uppercase letters) - 68^15 (combinations with no lowercase letters) - 84^15 (combinations with no numbers) - 62^15 (combinations with no special characters) + 42^15 (combinations with no uppercase letters and no lowercase letters) + 60^15 (combinations with no uppercase letters and no numbers) + 36^15 (combinations with no uppercase letters and no special characters) + 60^15 (combinations with no lowercase letters and no numbers) + 36^15 (combinations with no lowercase letters and no special characters) + 52^15 (combinations with no numbers and no special characters) - 24^15 (combinations with only uppercase letters) - 24^15 (combinations with only lowercase letters) - 10^15 (combinations with only numbers) - 32^15 (combinations with only special characters) ≈ 3.16228xE^29

Calculation without text:
94^15 - 68^15 - 68^15 - 84^15 - 62^15 + 42^15 + 60^15 + 36^15 + 60^15 + 36^15 + 52^15 - 24^15 - 24^15 - 10^15 - 32^15 ≈ 3.16228xE^29

- *N* number of possible passwords

Then *P* >= *T* x *G* / *N* (9.48682E-30 = 1 x 3 / 3.16228xE^29)

The probability of guessing a password in 1 minute is 9.48682E-30.

To provide additional password security, Comware 7.1 provides additional limits to the number of consecutive failed login attempts. If an FTP or VTY user fails authentication, the system adds the user to a password control blacklist. If a user fails to provide the correct password after the specified number of consecutive attempts, the system can take one of the following actions, based on the administrator's choice:

Blocks the user's login attempts until the user is manually removed from the password control blacklist.

Blocks the user's login attempts within a configurable period of time, and allows the user to log in again after the period of time elapses or the user is removed from the password control blacklist.

HPE Networking devices can also use certificate credentials using 2048 bit RSA keys and SHA-256; in such a case the security strength is 112 bits, so an attacker would have a 1 in 2^112 chance of a successful authentication which is much stronger than the one in a million chance required by FIPS 140-2. Certificate credentials using ECDSA keys with curves (P224, P-256, P-384, or P-521) and SHA algorithms (SHA-224, SHA-256, SHA-384, or SHA-512) are also available and provide a minimum of 112 bits security.

The users who try to log in or switch to a different user privilege level can be authenticated by RADIUS and TACACS+ Server. The minimum password length is 15 characters, and the maximum is 63. Therefore, for a 15 characters password, the probability of randomly guessing the correct sequence is one in 3.16228xE^29. The device (RADIUS client) and the RADIUS server use a shared key to authenticate RADIUS packets and encrypt user passwords exchanged between them. For more details, see RFC 2865: 3 Packet Format Authenticator field and 5.2 User-password.

- Role-based access control

  In Comware 7.1.045, the command and resource access permissions are assigned to roles.

  Users are given permission to access a set of commands and resources based on the users' user roles. Each user can have one or more roles. The user may alternate between authorized roles after first authenticating to the module.

6 Services, Key / CSP and Algorithm Tables

Assumptions, Assertions and Caveats

1. The preferred approach is to link Services to Keys/CSPs, Keys/CSPs to Algorithms and Algorithms to Services. When linkage is completed, there is a continuous loop among the three tables.
2. For linking the tables together, the goals are:
   - Confirm every Algorithm is listed at least once by a service.
   - Provide a direct mapping of the algorithm to each service that uses it.
   - Confirm every CSP is listed at least once by a service
   - Provide a direct mapping of the service to each CSP that it uses.
   - Provide a quick and easy way for the reviewer to navigate among the tables.

6.1 Services

Assumptions, Assertions and Caveats

1. The services table is the main focus of the validation. Preferably, it should be listed before the CSP and Algorithm tables.
2. Each service should map to the Key(s) / CSP(s) used by the service. It is not required that each service map to a Key / CSP.
3. Each service should be uniquely identifiable so the entries in the Algorithm Table can easily map to a service.

Services Table Column Definitions

1. Description

   Objective of this column is to provide a brief description of the service.

   - This column shall include a description of the service.
   - Where applicable the service description should describe the action being taken.

2. Input

   Objective of this column is to list the input to the service.

   - List the type of input such as command, configuration data or output of another service.

3. Output

   Objective of this column is to list the output of the service.

   - List the type of output generated by the service.

4. CSP Access

Objective of this column is to provide additional information about the CSP utilized by the service.

- Where applicable this column shall include the unique CSP identifier.
- The CSP identifier should contain a hyperlink to the entry in the CSP table.

5. Available to role

Objective of this column is to identify the role that can utilize the service.

- This column shall include the name of the role that can utilize the service.

Table 16 Crypto Officer Services

Description	Input	Output	CSP Access	Available to Role
View Device Status				
1. View currently running image version	Commands	Status of devices	None	Network-admin, level-15, level-9
2. View installed hardware components status and version	Commands	Status of devices	None	Network-admin, level-15, level-9
View Running Status				
3. View memory status, packet statistics, interface status, current running image version, current configuration, routing table, active sessions, temperature and SNMP MIB statistics.	Commands	Status of device functions	None	Network-admin, level-15, level-9

Perform Network Functions				
4. Network diagnostic service such as “ping”	Commands	Status of commands	None	Network-admin, level-15, level-9
5. Network connection service such as “SSHv2” client	Commands and configuration data	Status of commands and configuration data	CSP1-1 RSA Public key (read) CSP1-2 DSA Public key (read) CSP1-3 ECDSA Public key (read) CSP2-1 IPsec authentication keys (read/write/delete) CSP2-2 IPsec encryption keys (read/write/delete) CSP2-3 IPsec authentication keys (read) CSP2-4 IPsec encryption keys (read) CSP3-1 IKE pre-shared keys (read) CSP3-2 IKE RSA Authentication private Key (read) CSP3-3 IKE DSA Authentication private Key (read) CSP3-4 IKE Authentication key (read/write/delete) CSP3-5 IKE Encryption Key (read/write/delete) CSP3-6 IKE Diffie-Hellman Public Key (read/write/delete) CSP3-7 IKE Diffie-Hellman Private Key (read/write/delete) CSP4-1 IKEv2 pre-shared keys (read) CSP4-2 IKEv2 RSA Authentication private Key (read) CSP4-3 IKEv2 DSA Authentication private Key (read) CSP4-4 IKEv2 ECDSA Authentication private Key (read) CSP4-5 IKEv2 Authentication key (read/write/delete) CSP4-6 IKEv2 Encryption Key (read/write/delete) CSP4-7 IKEv2 Diffie-Hellman Public Key (read/write/delete) CSP4-8 IKEv2 Diffie-Hellman Private Key (read/write/delete) CSP4-9 IKEv2 ECDH Public Key (read/write/delete)	Network-admin, level-15, level-9

			CSP4-10 IKEv2 ECDH Private Key (read/write/delete) CSP5-1 SSH RSA Private key (read) CSP5-2 SSH ECDSA Private key (read) CSP5-3 SSH Diffie-Hellman Public Key (read/write/delete) CSP5-4 SSH Diffie-Hellman Private Key (read/write/delete) CSP5-5 SSH ECDH Public Key (read/write/delete) CSP5-6 SSH ECDH Private Key (read/write/delete) CSP5-7 SSH Session encryption Key (read/write/delete) CSP5-8 SSH Session authentication Key (read/write/delete) CSP9-1 SNMPv3 Authentication Key (read) CSP9-2 SNMPv3 Encryption Key (read) CSP7-1 DRBG entropy input (read/write/delete) CSP8-1 DRBG seed (read/write/delete) CSP8-2 DRBG V (read/write/delete) CSP8-3 DRBG Key (read/write/delete)	
6. Provide SSHv2 service.	Commands and configuration data	Status of commands and configuration data	CSP1-1 RSA Public key (read) CSP1-3 ECDSA Public key (read) CSP5-1 SSH RSA Private key (read) CSP5-2 SSH ECDSA Private key (read) CSP5-3 SSH Diffie-Hellman Public Key (read/write/delete) CSP5-4 SSH Diffie-Hellman Private Key (read/write/delete) CSP5-5 SSH ECDH Public Key (read/write/delete) CSP5-6 SSH ECDH Private Key (read/write/delete) CSP5-7 SSH Session encryption Key (read/write/delete) CSP5-8 SSH Session authentication Key (read/write/delete) CSP6-1 User Passwords (read/write/delete) CSP6-3 RADIUS shared secret keys (read) CSP6-4 TACACS+ shared secret keys (read)	Network-admin, level-15, level-9

			CSP7-1 DRBG entropy input (read/write/delete) CSP8-1 DRBG seed (read/write/delete) CSP8-2 DRBG V (read/write/delete) CSP8-3 DRBG Key (read/write/delete)	
7. Provide IKEv1/IKEv2/IPsec service to protect the session between the router and external server(e.g. Radius Server/Log Server)	Commands and configuration data	Status of commands and configuration data	CSP1-1 RSA Public key (read) CSP1-2 DSA Public key (read) CSP1-3 ECDSA Public key (read) CSP2-1 IPsec authentication keys (read/write/delete) CSP2-2 IPsec encryption keys (read/write/delete) CSP2-3 IPsec authentication keys (read) CSP2-4 IPsec encryption keys (read) CSP3-1 IKE pre-shared keys (read) CSP3-2 IKE RSA Authentication private Key (read) CSP3-3 IKE DSA Authentication private Key (read) CSP3-4 IKE Authentication key (read/write/delete) CSP3-5 IKE Encryption Key (read/write/delete) CSP3-6 IKE Diffie-Hellman Public Key (read/write/delete) CSP3-7 IKE Diffie-Hellman Private Key (read/write/delete) CSP4-1 IKEv2 pre-shared keys (read) CSP4-2 IKEv2 RSA Authentication private Key (read) CSP4-3 IKEv2 DSA Authentication private Key (read) CSP4-4 IKEv2 ECDSA Authentication private Key (read) CSP4-5 IKEv2 Authentication key (read/write/delete) CSP4-6 IKEv2 Encryption Key (read/write/delete) CSP4-7 IKEv2 Diffie-Hellman Public Key (read/write/delete) CSP4-8 IKEv2 Diffie-Hellman Private Key (read/write/delete) CSP4-9 IKEv2 ECDH Public Key (read/write/delete)	Network-admin, level-15, level-9

			CSP4-10 IKEv2 ECDH Private Key (read/write/delete) CSP7-1 DRBG entropy input (read/write/delete) CSP8-1 DRBG seed (read/write/delete) CSP8-2 DRBG V (read/write/delete) CSP8-3 DRBG Key (read/write/delete)	
8. Provide SNMPv3 service.	Commands and configuration data	Status of commands and configuration data	CSP9-1 SNMPv3 Authentication Key (read) CSP9-2 SNMPv3 Encryption Key (read) CSP7-1 DRBG entropy input (delete) CSP8-1 DRBG seed (delete) CSP8-2 DRBG V (delete) CSP8-3 DRBG Key (delete)	Network-admin, level-15, level-9
9. Initial Configuration setup (IP, hostname, DNS server)	Commands and configuration data	Status of commands and configuration data	None	Network-admin, level-15, level-9
10. Change the role	Commands and configuration data	Status of commands and configuration data	CSP6-1 User Passwords (read) CSP6-2 Super password (read) CSP6-3 RADIUS shared secret keys (read) CSP6-4 TACACS+ shared secret keys (read)	Network-admin, level-15, level-9
11. Reset and change the password of same/lower privilege user	Commands and configuration data	Status of commands and configuration data	CSP6-1 User Passwords (write/delete)	Network-admin, level-15, level-9
12. Maintenance of the super password	Commands and configuration data	Status of commands and configuration data	CSP6-2 Super password (write/delete)	Network-admin, level-15, level-9
13. Maintenance (create, destroy, import, export) of public key/private key/shared key	Commands and configuration data	Status of commands and configuration data	CSP1-1 RSA Public key (read/write/delete) CSP1-2 DSA Public key (read/write/delete) CSP1-3 ECDSA Public key (read/write/delete) CSP2-3 IPsec authentication keys (read/write/delete) CSP2-4 IPsec encryption keys (read/write/delete) CSP3-1 IKE pre-shared keys (read/write/delete) CSP3-2 IKE RSA Authentication private Key (read/write/delete)	Network-admin, level-15, level-9

			CSP3-3 IKE DSA Authentication private Key (read/write/delete) CSP4-1 IKEv2 pre-shared keys (read/write/delete) CSP4-2 IKEv2 RSA Authentication private Key (read/write/delete) CSP4-3 IKEv2 DSA Authentication private Key (read/write/delete) CSP4-4 IKEv2 ECDSA Authentication private Key (read/write/delete) CSP5-1 SSH RSA Private key (read/write/delete) CSP5-2 SSH ECDSA Private key (read/write/delete) CSP9-1 SNMPv3 Authentication Key (read/write/delete) CSP9-2 SNMPv3 Encryption Key (read/write/delete) CSP7-1 DRBG entropy input (read/write/delete) CSP8-1 DRBG seed (read/write/delete) CSP8-2 DRBG V (read/write/delete) CSP8-3 DRBG Key (read/write/delete)	
14. Management (create, delete, modify) of the user roles	Commands and configuration data	Status of commands and configuration data	None	Network-admin, level-15, level-9
15. Management of the access control rules for each role	Commands and configuration data	Status of commands and configuration data	None	Network-admin, level-15, level-9
16. Management (create, delete, modify) of the user account	Commands and configuration data	Status of commands and configuration data	CSP6-1 User Passwords (read/write/delete)	Network-admin, level-15, level-9
17. Management of the time	Commands and configuration data	Status of commands and configuration data	None	Network-admin, level-15, level-9
18. Maintenance (delete, modify) system start-up parameters	Commands and configuration data	Status of commands and configuration data	None	Network-admin, level-15, level-9
19. File operation (e.g. dir, copy, del)	Commands and configuration data	Status of commands and configuration data	CSP11-1 Firmware Signature (write/delete)	Network-admin, level-15, level-9
20. Shut down or Reboot the security appliance	Commands and configuration data	Status of commands and configuration data	CSP2-1 IPsec authentication keys (delete) CSP2-2 IPsec encryption keys (delete) CSP3-4 IKE Authentication key (delete)	Network-admin, level-15, level-9

			CSP3-5 IKE Encryption Key (delete) CSP4-5 IKEv2 Authentication key (delete) CSP4-6 IKEv2 Encryption Key (delete) CSP4-7 IKEv2 Diffie-Hellman Public Key (delete) CSP4-8 IKEv2 Diffie-Hellman Private Key (delete) CSP4-9 IKEv2 ECDH Public Key (delete) CSP4-10 IKEv2 ECDH Private Key (delete) CSP5-3 SSH Diffie-Hellman Public Key (delete) CSP5-4 SSH Diffie-Hellman Private Key (delete) CSP5-5 SSH ECDH Public Key (delete) CSP5-6 SSH ECDH Private Key (delete) CSP5-7 SSH Session encryption Key (delete) CSP5-8 SSH Session authentication Key (delete) CSP7-1 DRBG entropy input (delete) CSP8-1 DRBG seed (delete) CSP8-2 DRBG V (delete) CSP8-3 DRBG Key (delete) CSP11-1 Firmware Signature (read)	
21. Maintenance of IKEv1/IKEv2/IPsec.	Commands and configuration data	Status of commands and configuration data	CSP1-1 RSA Public key (read/write/delete) CSP1-2 DSA Public key (read/write/delete) CSP1-3 ECDSA Public key (read/write/delete) CSP2-3 IPsec authentication keys (read/write/delete) CSP2-4 IPsec encryption keys (read/write/delete) CSP3-1 IKE pre-shared keys (read/write/delete) CSP3-2 IKE RSA Authentication private Key (read/write/delete) CSP3-3 IKE DSA Authentication private Key (read/write/delete) CSP4-1 IKEv2 pre-shared keys (read/write/delete) CSP4-2 IKEv2 RSA Authentication private Key (read/write/delete) CSP4-3 IKEv2 DSA Authentication private Key (read/write/delete) CSP4-4 IKEv2 ECDSA Authentication private Key (read/write/delete)	Network-admin, level-15, level-9

22. Maintenance of SNMPv3	Commands and configuration data	Status of commands and configuration data	CSP9-1 SNMPv3 Authentication Key (read/write/delete) CSP9-2 SNMPv3 Encryption Key (read/write/delete)	Network-admin, level-15, level-9
23. Maintenance of SSHv2	Commands and configuration data	Status of commands and configuration data	CSP1-1 RSA Public key (read/write/delete) CSP1-3 ECDSA Public key (read/write/delete) CSP5-1 SSH RSA Private key (read/write/delete) CSP5-2 SSH ECDSA Private key (read/write/delete) CSP5-7 SSH Session encryption Key (read/write/delete) CSP5-8 SSH Session authentication Key (read/write/delete)	Network-admin, level-15, level-9
24. Perform self-test	Commands and configuration data	Status of commands and configuration data	None	Network-admin, level-15, level-9
25. Displaying and maintaining security log files	Commands and configuration data	Status of commands and configuration data	None	security-audit
Perform Configuration Functions				
26. Save configuration	Commands and configuration data	Status of commands and configuration data	None	Network-admin, level-15, level-9
27. Management of information center	Commands and configuration data	Status of commands and configuration data	None	Network-admin, level-15, level-9
28. Define network interfaces and settings	Commands and configuration data	Status of commands and configuration data	None	Network-admin, level-15, level-9
29. Set the protocols the routers will support(e.g. SFTP server, SSHv2 server)	Commands and configuration data	Status of commands and configuration data	None	Network-admin, level-15, level-9
30. Enable interfaces and network services	Commands and configuration data	Status of commands and configuration data	None	Network-admin, level-15, level-9
31. Management of access control scheme	Commands and configuration data	Status of commands and configuration data	None	Network-admin, level-15, level-9

32. Config managing security log files and security log file system	Commands and configuration data	Status of commands and configuration data	None	security-audit
33. Enable/Disable FIPS mode of operation	Commands and configuration data	Status of commands and configuration data	All private and session keys are zeroized when switching between FIPS and non-FIPS modes	Network-admin, level-15
34. Load firmware[2]	Commands and configuration data	Status of commands and configuration data	CSP11-1 Firmware Signature (read)	Network-admin, level-15

Table 17 User Services

Description	Input	Output	CSP Access	Available to Role
View Device Status				
1. View currently running image version; 2. View installed hardware components status and version	Commands	Status of devices	None	network-operator level-1
View Running Status				
3. View memory status, packet statistics, interface status, current running image version, current configuration, routing table, active sessions, temperature and SNMP MIB statistics.	Commands	Status of device functions	None	network-operator level-1
Perform Network Functions				
4. Network diagnostic service such as “ping”;	Commands and	Status of	None	Level-0,

[2] New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and requires a separate FIPS 140-2 validation.

Description	Input	Output	CSP Access	Available to Role
	configuration data	commands and configuration data		Level-1
5. Network connection service such as “SSHv2” client.	Commands and configuration data	Status of commands and configuration data	CSP1-1 RSA Public key (read) CSP1-2 DSA Public key (read) CSP1-3 ECDSA Public key (read) CSP2-1 IPsec authentication keys (read/write/delete) CSP2-2 IPsec encryption keys (read/write/delete) CSP2-3 IPsec authentication keys (read) CSP2-4 IPsec encryption keys (read) CSP3-1 IKE pre-shared keys (read) CSP3-2 IKE RSA Authentication private Key (read) CSP3-3 IKE DSA Authentication private Key (read) CSP3-4 IKE Authentication key (read/write/delete) CSP3-5 IKE Encryption Key (read/write/delete) CSP3-6 IKE Diffie-Hellman Public Key (read/write/delete) CSP3-7 IKE Diffie-Hellman Private Key (read/write/delete) CSP4-1 IKEv2 pre-shared keys (read) CSP4-2 IKEv2 RSA Authentication private Key (read) CSP4-3 IKEv2 DSA Authentication private Key (read) CSP4-4 IKEv2 ECDSA Authentication private Key (read) CSP4-5 IKEv2 Authentication key (read/write/delete) CSP4-6 IKEv2 Encryption Key (read/write/delete) CSP4-7 IKEv2 Diffie-Hellman Public Key (read/write/delete) CSP4-8 IKEv2 Diffie-Hellman Private Key (read/write/delete) CSP4-9 IKEv2 ECDH Public Key (read/write/delete) CSP4-10 IKEv2 ECDH Private Key (read/write/delete)	Level-0, Level-1

Description	Input	Output	CSP Access	Available to Role
			CSP5-1 SSH RSA Private key (read) CSP5-2 SSH ECDSA Private key (read) CSP5-3 SSH Diffie-Hellman Public Key (read/write/delete) CSP5-4 SSH Diffie-Hellman Private Key (read/write/delete) CSP5-5 SSH ECDH Public Key (read/write/delete) CSP5-6 SSH ECDH Private Key (read/write/delete) CSP5-7 SSH Session encryption Key (read/write/delete) CSP5-8 SSH Session authentication Key (read/write/delete) CSP9-1 SNMPv3 Authentication Key (read) CSP9-2 SNMPv3 Encryption Key (read) CSP7-1 DRBG entropy input (delete) CSP8-1 DRBG seed (delete) CSP8-2 DRBG V (delete) CSP8-3 DRBG Key (delete)	
6. Provide SSHv2 service.	Commands and configuration data	Status of commands and configuration data	CSP1-1 RSA Public key (read) CSP1-3 ECDSA Public key (read) CSP5-1 SSH RSA Private key (read) CSP5-2 SSH ECDSA Private key (read) CSP5-3 SSH Diffie-Hellman Public Key (read/write/delete) CSP5-4 SSH Diffie-Hellman Private Key (read/write/delete) CSP5-5 SSH ECDH Public Key (read/write/delete) CSP5-6 SSH ECDH Private Key (read/write/delete) CSP5-7 SSH Session encryption Key (read/write/delete) CSP5-8 SSH Session authentication Key (read/write/delete) CSP6-1 User Passwords (read/write/delete) CSP6-3 RADIUS shared secret keys (read) CSP6-4 TACACS+ shared secret keys (read) CSP7-1 DRBG entropy input (delete)	Level-0, Level-1

Description	Input	Output	CSP Access	Available to Role
			CSP8-1 DRBG seed (delete) CSP8-2 DRBG V (delete) CSP8-3 DRBG Key (delete)	
7. Provide IKEv1/IKEv2/IPsec service to protect the session between the router and external server(e.g. Radius Server/Log Server)	Commands and configuration data	Status of commands and configuration data	CSP1-1 RSA Public key (read) CSP1-2 DSA Public key (read) CSP1-3 ECDSA Public key (read) CSP2-1 IPsec authentication keys (read/write/delete) CSP2-2 IPsec encryption keys (read/write/delete) CSP2-3 IPsec authentication keys (read) CSP2-4 IPsec encryption keys (read) CSP3-1 IKE pre-shared keys (read) CSP3-2 IKE RSA Authentication private Key (read) CSP3-3 IKE DSA Authentication private Key (read) CSP3-4 IKE Authentication key (read/write/delete) CSP3-5 IKE Encryption Key (read/write/delete) CSP3-6 IKE Diffie-Hellman Public Key (read/write/delete) CSP3-7 IKE Diffie-Hellman Private Key (read/write/delete) CSP4-1 IKEv2 pre-shared keys (read) CSP4-2 IKEv2 RSA Authentication private Key (read) CSP4-3 IKEv2 DSA Authentication private Key (read) CSP4-4 IKEv2 ECDSA Authentication private Key (read) CSP4-5 IKEv2 Authentication key (read/write/delete) CSP4-6 IKEv2 Encryption Key (read/write/delete) CSP4-7 IKEv2 Diffie-Hellman Public Key (read/write/delete) CSP4-8 IKEv2 Diffie-Hellman Private Key (read/write/delete) CSP4-9 IKEv2 ECDH Public Key (read/write/delete)	Level-0, Level-1

Description	Input	Output	CSP Access	Available to Role
			CSP4-10 IKEv2 ECDH Private Key (read/write/delete) CSP7-1 DRBG entropy input (read/write/delete) CSP8-1 DRBG seed (read/write/delete) CSP8-2 DRBG V (read/write/delete) CSP8-3 DRBG Key (read/write/delete)	
8. Provide SNMPv3 service.	Commands and configuration data	Status of commands and configuration data	CSP9-1 SNMPv3 Authentication Key (read) CSP9-2 SNMPv3 Encryption Key (read) CSP7-1 DRBG entropy input (read/write/delete) CSP8-1 DRBG seed (read/write/delete) CSP8-2 DRBG V (read/write/delete) CSP8-3 DRBG Key (read/write/delete)	Level-0, Level-1

6.1.1 **Unauthenticated Services**

Description	Input	Output	CSP Access
1. Cycle the power on the router	Pulling the plug or flipping the power switch	Device powers on/off	None[3]
2. View currently running image version	View log data on remote server	Image version	None
3. View installed hardware components status and version	Visual inspection	Component status and version	None
4. View memory status, packet statistics, interface status, current running image version, current configuration, routing table, active sessions, temperature and SNMP MIB statistics	View SNMP data on remote server	Device status	None

[3] All ephemeral keys are zeroized after power loss. See CSPs referenced by Crypto Officer Service #20.

6.1.2 **Non-Approved Services**

The HPE network routers support the following non-approved services:

- Internet Key Exchange (IKE) or Internet Protocol Security (IPsec) with AES-XCBC-MAC, Camellia, DES, Triple-DES, MD5, HMAC-MD5, Diffie-Hellman (<2048-bits), RSA (< 2048-bits), DSA (< 2048-bits), ECDSA (<224-bits).
- Perform Network Time Protocol (NTP) service.
- Perform Secure Socket Layer (SSL) 3.0 or Transport Layer Security (TLS) 1.0, 1.1, 1.2.
- Perform Secure Shell version 1.x.
- Perform Secure Shell version 2.0 with DES, Triple-DES, MD5, HMAC-MD5, Diffie-Hellman (<2048-bits), RSA (< 2048-bits), DSA (<2048-bits), ECDSA (<224-bits)
- Perform Telnet

6.2 **Critical Security Parameters**

[4]Critical security parameter (CSP): security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and PINs) whose disclosure or modification can compromise the security of a cryptographic module.[5]

Assumptions, Assertions and Caveats

1. Preferably, the Key / CSP Table should be listed after the Services Table.
2. Each Key(s) / CSP(s) must be mapped to by a service. A Key / CSP cannot exist unless associated with a service.
3. Each Key / CSP should be uniquely identifiable so the entries in the Services Table can easily map to a Key / CSP.
4. The DH key pairs should be 2 entries in the table. One for the public key and one for the private key – since the key lengths are different
   - Each public key should be in its own row.
   - Each private key should be in its own row.
5. For all RSA keys, state whether it is used for key transport or signature generation/verification.
   - Key transport should be in its own row.
   - Signature generation/verification should be in its own row.
6. Where possible, group Key / CSP together e.g. Keys associated with a protocol should be grouped together.

KEY / CSP Table Column Definitions

1. Key / CSP #

   Unique identifier of CSP

2. Key or CSP Name

   Objective of this column is the list the type of key or CSP used by the cryptographic module.

   - To avoid confusion wherever possible it is recommended that the name of the key/CSP be consistent with a recognized industry standard such as ISO, IETF or NIST Special Publication.

[4] FIPS Pub 140-2
[5] In Comware, CSPs generated in FIPS mode cannot be used in non-FIPS mode, and vice versa.

3. Key/CSP Type & Algorithm Link

   Objective of this column is to provide additional information about the CSP.

   - Where applicable this column shall include the type of key/CSP, algorithm(s) (including reference to FIPS or NIST SP).
   - The Algorithm link points to the Algorithm in the Algorithm table the Key/CSP uses.

4. Key size

   Size of the key used by the CSP.

5. Use

   The objective of this column is to provide information on how the key is used during cryptographic module operation.

   - This column should contain a short description of the Key/CSP.
   - It is important that each CSP is mapped directly **from** an Approved service that the cryptographic module performs.
   - For all RSA keys, this column shall specify whether it is used for key transport or signature generation/verification

6. Generation/Input

   The objective of this column is to specify how and when the CSP is generated, derived or enters the module.

   - If the CSP is generated or derived, this column shall specify the function or technique responsible.
   - If the CSP is entered, the column shall specify if the CSP is entered electronically or manually.
   - The column shall specify if it is stored encrypted or in plaintext form.
   - If the CSP is ephemeral this column shall specify conditions upon which it is generated (A cryptographic key is called ephemeral if it is generated for each execution of a key establishment process.).

7. Storage

   The objective of this column is to specify where the CSP is stored during cryptographic module operation.

   - The column shall also state the location and type of storage.
   - The column shall state if the CSP is persistent, ephemeral or hardcoded.

- The column shall specify if it is stored encrypted or in plaintext form.
- The column shall specify if only a pointer or reference to the CSP is stored or the actual CSP.

8. Output

   The objective of this column is to specify if the CSP can be output from the cryptographic module.

   - If the CSP can be output, the column shall specify how it can be output.
   - If the CSP can be output, the column shall specify if it is encrypted or plaintext form.

9. Zeroization

   The objective of this column is to provide details on how the CSP shall be zeroized.

   - All possible zeroization techniques for the CSP shall be listed.

Table 18 Critical Security Parameters

#	Key / CSP Name	Key / CSP Type Algorithm Link	Key Size	Use	Generation[6] / Input	Storage	Output	Zeroization
Public key management								
CSP1-1	RSA public key	RSA RSA-1 RSA-2 RSA-3 RSA-4	2048 bits	Identity certificates for the security appliance itself and also used in IPsec and SSH	Electronically generated OR Externally generated; input in ciphertext	FLASH (cipher text / AES256)	Plaintext	Using CLI command to zeroize.

[6] For all keys marked as "Electronically generated", the resulting symmetric key or the generated seed to be used in the asymmetric key generation is an unmodified output from the DRBG.

#	Key / CSP Name	Key / CSP Type Algorithm Link	Key Size	Use	Generation[6] / Input	Storage	Output	Zeroization
CSP1-2	DSA public key	DSA DSA-1 DSA-2 DSA-3 DSA-4	2048 bits	Identity certificates for the security appliance itself and also used in IPsec and SSH	Electronically generated OR Externally generated; input in ciphertext	FLASH (cipher text / AES256)	Plaintext	Using CLI command to zeroize
CSP1-3	ECDSA public key	ECDSA ECDSA-1 ECDSA-2 ECDSA-3	NIST P256, P384, P521	Identity certificates for the security appliance itself and also used in IPsec and SSH.	Electronically generated OR Externally generated; input in ciphertext	FLASH (cipher text / AES256)	Plaintext	Using CLI command to zeroize
IPsec								
CSP2-1	IPsec authentication keys	HMAC-SHA1-96 HMAC-SHA-256-128 HMAC-SHA-384-192 HMAC-SHA-512-256 GMAC-128 GMAC-192 GMAC-256 HMAC-1	HMAC: 160 bits 256 bits 384 bits 512 bits GMAC: 128 bits 192 bits	Used to authenticate the IPsec traffic	Electronically generated	RAM (plain text)	No	Automatically when session expires.

#	Key / CSP Name	Key / CSP Type Algorithm Link	Key Size	Use	Generation[6] / Input	Storage	Output	Zeroization
		HMAC-2 HMAC-3 AES-1 AES-2 AES-3	256 bits					
CSP2-2	IPsec encryption keys	AES AES-1 AES-2 AES-3	128 bits, 192 bits, 256 bits	Used to encrypt the IPsec traffic	Electronically generated	RAM (plain text)	No	Automatically when session expires.
CSP2-3	IPsec authentication keys	HMAC-SHA1-96 HMAC-SHA-256-128 HMAC-SHA-384-192 HMAC-SHA-512-256 GMAC-128 GMAC-192 GMAC-256	HMAC: 160 bits 256 bits 384 bits 512 bits GMAC: 128 bits 192 bits 256 bits	Used to authenticate the IPsec traffic	Manually entered by the Crypto-Officer	FLASH (cipher text / AES-CTR 256) and RAM (plain text)	Encrypted	Keys will be zeroized using CLI commands "**undo sa hex-key authentication …**" and " **save**",
		HMAC-1 HMAC-2 HMAC-3 AES-1 AES-2 AES-3						

#	Key / CSP Name	Key / CSP Type Algorithm Link	Key Size	Use	Generation[6] / Input	Storage	Output	Zeroization
CSP2-4	IPsec encryption keys	AES AES-1 AES-2 AES-3	128 bits, 192 bits, 256 bits	Used to encrypt the IPsec traffic	Manually entered by the Crypto-Officer	FLASH (cipher text / AES-CTR 256) and RAM (plain text)	Encrypted	Keys will be zeroized using CLI commands "**undo sa hex-key encryption …**" and " **save**",
IKEv1								
CSP3-1	IKE pre-shared keys	Shared Secret AES-3	15 ~ 128 bytes	Used for authentication during IKE	Manually entered by the Crypto-Officer	FLASH(cipher text/ AES-CTR-256) and RAM (cipher text/ AES-CTR-256)	Encrypted	Using CLI command to zeroize
CSP3-2	IKE RSA Authentication private Key	RSA RSA-1 RSA-3 RSA-4	2048 bits	private key used for IKE protocol during the handshake	Electronically generated OR Externally generated; input in ciphertext	RAM (plain text)	No	Automatically when handshake finishing
CSP3-3	IKE DSA Authentication private Key	DSA DSA-3 DSA-4	256 bits	private key used for IKE protocol during the handshake	Electronically generated OR Externally generated; input in ciphertext	RAM (plain text)	No	Automatically when handshake finishing
CSP3-4	IKE Authentication key	HMAC-SHA1, HMAC-SHA256 HMAC-HA384,	160 bits 256 bits 384 bits,	Used to authenticate IKE negotiations	Electronically generated	RAM (plain text)	No	Automatically when session expires.

#	Key / CSP Name	Key / CSP Type Algorithm Link	Key Size	Use	Generation[6] / Input	Storage	Output	Zeroization
		HMAC-SHA512 HMAC-2 HMAC-3	512 bits					
CSP3-5	IKE Encryption Key	AES AES-3	128 bits, 192 bits, 256 bits	Used to encrypt IKE negotiations	Electronically generated	RAM (plain text)	No	Automatically when session expires.
CSP3-6	IKE Diffie-Hellman Public Key	DH CVL-1	2048 bits	Key agreement for IKE	Electronically generated	RAM (plain text)	No	Automatically when handshake finishing
CSP3-7	IKE Diffie-Hellman Private Key	DH CVL-1	DH Group 14: 2048 bits DH Group 24: 256 bits	Key agreement for IKE	Electronically generated	RAM (plain text)	No	Automatically when handshake finishing
IKEv2								
CSP4-1	IKEv2 pre-shared keys	Shared Secret AES-3	15 ~ 128 bytes	Used for authentication during IKEv2	Manually entered by the Crypto-Officer	FLASH(cipher text/ AES-CTR-256) and RAM (cipher text/ AES-CTR-256)	Encrypted	Using CLI command to zeroize
CSP4-2	IKEv2 RSA Authentication private Key	RSA RSA-1 RSA-3 RSA-4	2048 bits	private key used for IKEv2 protocol during the handshake	Electronically generated OR Externally generated; input in ciphertext	RAM (plain text)	No	Automatically when handshake finishing

#	Key / CSP Name	Key / CSP Type Algorithm Link	Key Size	Use	Generation[6] / Input	Storage	Output	Zeroization
CSP4-3	IKEv2 DSA Authentication private Key	DSA DSA-3 DSA-4	256 bits	private key used for IKEv2 protocol during the handshake	Electronically generated OR Externally generated; input in ciphertext	RAM (plain text)	No	Automatically when handshake finishing
CSP4-4	IKEv2 ECDSA Authentication private Key	ECDSA ECDSA-2 ECDSA-3	ECDSA:P-256, P-384, P-521	private key used for IKEv2 protocol during the handshake	Electronically generated OR Externally generated; input in ciphertext	RAM (plain text)	No	Automatically when handshake finishing
CSP4-5	IKEv2 Authentication key	HMAC-SHA1, HMAC-SHA256 HMAC-SHA384, HMAC-SHA512 HMAC-2 HMAC-3	160 bits 256 bits 384 bits, 512 bits	Used to authenticate IKEv2 negotiations	Electronically generated	RAM (plain text)	No	Automatically when session expires.
CSP4-6	IKEv2 Encryption Key	AES AES-3	128 bits, 192 bits, 256 bits	Used to encrypt IKEv2 negotiations	Electronically generated	RAM (plain text)	No	Automatically when session expires.
CSP4-7	IKEv2 Diffie-Hellman Public Key	DH CVL-1	2048 bits	Key agreement for IKEv2	Electronically generated	RAM (plain text)	No	Automatically when handshake finishing

#	Key / CSP Name	Key / CSP Type Algorithm Link	Key Size	Use	Generation[6] / Input	Storage	Output	Zeroization
CSP4-8	IKEv2 Diffie-Hellman Private Key	DH CVL-1	DH Group 14: 2048 bits DH Group 24: 256 bits	Key agreement for IKEv2	Electronically generated	RAM (plain text)	No	Automatically when handshake finishing
CSP4-9	IKEv2 ECDH Public Key	ECDH CVL-2	P-256, P-384, P-521	Key agreement for IKEv2	Electronically generated	RAM (plain text)	No	Automatically when handshake finishing
CSP4-10	IKEv2 ECDH Private Key	ECDH CVL-2	P-256: 256 bits P-384: 384 bits	Key agreement for IKEv2	Electronically generated	RAM (plain text)	No	Automatically when handshake finishing
SSH								
CSP5-1	SSH RSA Private key	RSA RSA-1 RSA-3 RSA-4	2048 bits	private key used for SSH protocol	Electronically generated OR Externally generated; input in ciphertext	RAM(plain text)	No	Automatically when handshake finishing
CSP5-2	SSH ECDSA Private key	ECDSA ECDSA-2 ECDSA-3	P-256, P-384	private key used for SSH protocol	Electronically generated OR Externally generated; input in ciphertext	RAM(plain text)	No	Automatically when handshake finishing

#	Key / CSP Name	Key / CSP Type Algorithm Link	Key Size	Use	Generation[6] / Input	Storage	Output	Zeroization
CSP5-3	SSH Diffie-Hellman Public Key	DH CVL-1	2048 bits	Public key agreement for SSH sessions.	Electronically generated	RAM (plain text)	No	Automatically when handshake finishing
CSP5-4	SSH Diffie-Hellman Private Key	DH CVL-1	2048 bits	Private key agreement for SSH sessions.	Electronically generated	RAM (plain text)	No	Automatically when handshake finishing
CSP5-5	SSH ECDH Public Key	ECDH CVL-2	P-256, P-384	Public key agreement for SSH sessions.	Electronically generated	RAM (plain text)	No	Automatically when handshake finishing
CSP5-6	SSH ECDH Private Key	ECDH CVL-2	P-256, P-384	Private key agreement for SSH sessions.	Electronically generated	RAM (plain text)	No	Automatically when handshake finishing
CSP5-7	SSH Session encryption Key	AES AES-3	128 bits, 192 bits, 256 bits	SSH session symmetric key	Electronically generated	RAM (plain text)	No	Automatically when SSH session terminated
CSP5-8	SSH Session authentication Key	HMAC HMAC-2 HMAC-3	160 bits 256 bits 512 bits	SSH session authentication key	Electronically generated	RAM (plain text)	No	Automatically when SSH session terminated
Authentication								
CSP6-1	User Passwords	Secret AES-3	15 ~ 63 bytes	Used to authenticate the administrator login.	Manually entered by the Crypto-Officer	FLASH (cipher text / AES256)	Encrypted	Using CLI command to zeroize

#	Key / CSP Name	Key / CSP Type Algorithm Link	Key Size	Use	Generation[6] / Input	Storage	Output	Zeroization
CSP6-2	Super password	Secret AES-3	15 ~ 63 bytes	Used to authenticate the user role.	Manually entered by the Crypto-Officer	FLASH (cipher text / AES256)	Encrypted	Using CLI command to zeroize
CSP6-3	RADIUS shared secret keys	Shared Secret AES-3	15 ~ 64 bytes	Used for authenticating the RADIUS server to the security appliance and vice versa.	Manually entered by the Crypto-Officer	FLASH (cipher text / AES256)	Encrypted	Using CLI command to zeroize
CSP6-4	TACACS+ shared secret keys	Shared Secret AES-3	15~255 bytes	Used for authenticating the TACACS+ server to the security appliance and vice versa.	Manually entered by the Crypto-Officer	FLASH (cipher text / AES256)	Encrypted	Using CLI command to zeroize
Entropy								
CSP7-1	DRBG entropy input	SP 800-90A CTR_DRBG DRBG-1	256 bits	Entropy source used to construct seed	Electronically generated	RAM (plaintext)	No	Resetting or rebooting the security appliance
Random Bits Generation								
CSP8-1	DRBG seed	SP 800-90A CTR_DRBG DRBG-1	384 bits	Input to the DRBG that determines the internal state of the DRBG	Electronically generated	RAM (plaintext)	Never exits the module	Resetting or rebooting the security appliance
CSP8-2	DRBG V	SP 800-90A CTR_DRBG	128 bits	Generated by entropy source via the	Electronically generated	RAM (plaintext)	Never exits the module	Resetting or rebooting the security appliance

#	Key / CSP Name	Key / CSP Type Algorithm Link	Key Size	Use	Generation[6] / Input	Storage	Output	Zeroization
		DRBG-1		CTR_DRBG derivation function. It is stored in DRAM with plaintext form				
CSP8-3	DRBG Key	SP 800-90A CTR_DRBG DRBG-1	256 bits	AES key used for SP 800-90A CTR_DRBG	Electronically generated	RAM (plaintext)	Never exits the module	Resetting or rebooting the security appliance
SNMPv3								
CSP9-1	SNMPv3 Authentication Key	HMAC-SHA1 HMAC-3	160 bits	Used to verify SNMPv3 packet.	Manually entered by the Crypto-Officer	FLASH (cipher text / AES256) RAM (plain text)	Encrypted	Using CLI command to zeroize
CSP9-2	SNMPv3 Encryption Key	AES AES-3	128 bits	Used to encrypt SNMPv3 packet.	Manually entered by the Crypto-Officer	FLASH (cipher text / AES256) RAM (plain text)	Encrypted	Using CLI command to zeroize
System KEK								
CSP10-1	Key encrypting key	AES AES-1 AES-2 AES-3	256 bits	Used to encrypt all private key, user password, and pre-shared key stored on internal storage. The KEK is generated using random bytes	Electronically generated	RAM (plain text)	No	Zeroized when Resetting or rebooting the security appliance

#	Key / CSP Name	Key / CSP Type Algorithm Link	Key Size	Use	Generation[6] / Input	Storage	Output	Zeroization
System Firmware								
CSP11-1	Firmware Signature	RSA	2048 bits	Factory signature used to verify Comware 7 firmware.	Generated by HPE Comware 7 Build Team	FLASH (binary images)	Binary image	Upon deletion of binary image.

6.3 **Approved Algorithms**

Assumptions, Assertions and Caveats

1. Each instantiation of the algorithm should be in a separate table
   - e.g. kernel, firmware, accelerators
   - e.g. chassis / controller
2. Each instantiation of the algorithm should be uniquely identifiable so the Key / CSP can easily map to an algorithm.
3. Include a reference to the FIPS 140-2 approved standard for each algorithm. One example is to use a footnote.
4. The ECB mode is required for all other AES modes. The ECB mode should be listed as not used by the module if ECB is only used to support the other modes. If the ECB mode is used by one or more services, it should be listed as available. Although ECB is the basis for all other AES modes, it is latent functionality if there is no service that uses it.
5. Each instantiation of the algorithm must map to the service that uses it.
6. To expedite the review process, each instantiation of the algorithm should have a hyperlink to the CAVP page that contains the certification listing.
7. It is important to identify which algorithms are used by the module and which are not. All functionality listed on the CAVP certificate should be detailed somewhere in the tables, footnotes, or text of the Security Policy. If all of the functionality is used by the module, then all algorithm functionality belongs in the tables. If some functionality is not used by the module, then the author should determine the best to convey that to the reader. (The Tables use footnotes. But there are other ways to convey this information.)

Algorithm Table Column Definitions

1. Algorithm #

   Unique identifier of the algorithm. Each instantiation should be uniquely identified.

2. CAVP Certificate

   Objective of this column is identify the CAVP certificate.

   - The certificate number should be listed.
   - A hyperlink should be create to the CAVP website to the certificate number.

3. Algorithm

   Objective of this column is identify the Algorithm in use.

   - The algorithm name should be consistent with the names list on the Cryptographic Algorithm Validation Program (CAVP) website.

- The acronym may be used instead of the full name.
- Include a reference to the FIPS 140-2 approved standard for each algorithm.

4. Mode / Method

   Objective of this column is identify the Mode / Method used by the algorithm.

5. Key Lengths, Curves or Moduli

   Objective of this column is identify the Key Lengths, Curves or Moduli used by the algorithm.

6. Use

   Objective of this column is identify the use of the algorithm.

7. Service that uses Algorithm

   Objective of this column is identify the services that use the algorithm.

   - A cross reference should be made to the unique identifier in a services table
   - The cross reference should contain a hyperlink to the entry in a services table.
   - The relationship of algorithm to service maybe one-to-one, one-to-many, or many-to-many.

Table 19 Comware V7 Kernel – Approved Algorithms

#	CAVP Certificate	Algorithm	Mode/ Method	Key Lengths, Curves or Moduli	Use	Service that uses Algorithm
AES-1	4096	AES[7]	ECB[8], CBC[9], CTR, GCM[10], GMAC	128, 192, 256	Kernel – Data Encryption/ Decryption	**Crypto Officer Services** (7, 21, 24) **User Services** (7)
HMAC-1[11]	2676	HMAC[12]	HMAC SHA-1, HMAC-SHA-1-96	160	Kernel - Message Authentication	**Crypto Officer Services** (7, 21, 24) **User Services** (7)
SHS-1[11]	3372	SHS[13]	SHA-1		Kernel – Message Digest	**Crypto Officer Services** (7, 21, 24) **User Services** (7)
TDES-1[14]	2239	Triple-DES[15]	TECB[16], TCBC	192	Self-tests	**Crypto Officer Services** (24)

[7] FIPS 197

[8] Not used by the module

[9] SP 800-38A

[10] The module's AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 6071 for IPsec and RFC 5288 for TLS. The module uses a 96-bit IV, which is comprised of a 4 byte salt unique to the crypto session and 8 byte monotonically increasing counter. The module generates new AES-GCM keys if the module loses power.

[11] Although the certification supports additional hash sizes. Only those listed are used by the module.

[12] FIPS 198-1

[13] FIPS 180-4

[14] Although the certification contains Triple-DES, Triple-DES is used only for self-tests in the approved mode.

[15] SP 800-67rev1

[16] Not used by the module

#	CAVP Certificate	Algorithm	Mode/ Method	Key Lengths, Curves or Moduli	Use	Service that uses Algorithm
						User Services None

Table 20 Comware V7 HW Accelerators – Approved Algorithms

#	CAVP Certificate	Algorithm	Mode/ Method	Key Lengths or Curves	Use	Service that uses Algorithm
AES-2	4094	AES[17]	ECB[18], CBC, CTR, GCM[19], GMAC	128, 192, 256	Data Encryption/ Decryption	**Crypto Officer Services** (5, 6, 7, 8, 13, 14, 15, 16, 24) **User Services** 5, 6, 7, 8
HMAC-2	2674	HMAC[20]	HMAC SHA-1, HMAC-SHA-1-96, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	160, 256, 384, 512	Message Authentication	**Crypto Officer Services** (5, 6, 7, 8, 13, 14, 15, 16, 24) **User Services** 5, , 6, 7, 8
SHS-2	3370	SHS[21]	SHA-1, SHA-256, SHA-384, SHA-512		Message Digest	**Crypto Officer Services** (5, 6, 7, 8, 13, 14, 15, 16, 24) **User Services** 5, 6, 7, 8

[17] FIPS 197
[18] Not used by the module
[19] SP 800-38A, SP 800-38D
The module's AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 6071 for IPsec and RFC 5288 for TLS. The module uses a 96-bit IV, which is comprised of a 4 byte salt unique to the crypto session and 8 byte monotonically increasing counter. The module generates new AES-GCM keys if the module loses power.
[20] FIPS 198-1
[21] FIPS 180-4

#	CAVP Certificate	Algorithm	Mode/ Method	Key Lengths or Curves	Use	Service that uses Algorithm
TDES-2[22]	2237	Triple-DES[23]	TECB[24], TCBC	192	Self-tests	**Crypto Officer Services** (24) **User Services** None

Table 21 Comware V7 HW Accelerators - Allowed Algorithms

Algorithm	Caveat	Use	Service that uses Algorithm
None			**Crypto Officer Services** (none) **User Services** (none)

[22] Although the certification contains Triple-DES it is used only for self-tests in the approved mode.
[23] SP 800-67rev1
[24] Not used by the module

Table 22 Comware V7 Firmware – Approved Algorithms

#	CAVP Certificate	Algorithm	Mode/ Method	Key Lengths or Curves	Use	Service that uses Algorithm
AES-3	4091	AES[25]	ECB[26], CBC, CTR, GCM[27], GMAC, KW[28]	128, 192, 256	Data Encryption/ Decryption	**Crypto Officer Services** (5, 6, 7, 8, 11, 12, 13, 21, 22, 23, 24) **User Services** (5, 6, 7, 8)
CVL-1[29]	908	CVL[30] IKEv1, IKEv2 TLS 1.0/1.1[31] SSH, SNMPv3 KDFs			Key Derivation	**Crypto Officer Services** (5, 6, 7, 8, 24) **User Services** (5, 6, 7, 8)
DRBG-1	1229	DRBG[32]	CTR (AES-256)		Deterministic Random Bit Generation	**Crypto Officer Services** (5, 6, 7, 8, 13, 24)

[25] FIPS 197, SP 800-38A, SP 800-38D

[26] Not used by the module

[27] The module's AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 6071 for IPsec and RFC 5288 for TLS. The module uses a 96-bit IV, which is comprised of a 4 byte salt unique to the crypto session and 8 byte monotonically increasing counter. The module generates new AES-GCM keys if the module loses power.

[28] Not used by the module

[29] Component Validation: the protocols covered under this certificate have not been reviewed or tested by the CAVP or CMVP

[30] SP 800-135rev1

[31] Although the certification contains TLS, it is not used in this version of Comware in the approved mode.

[32] SP 800-90A

#	CAVP Certificate	Algorithm	Mode/ Method	Key Lengths or Curves	Use	Service that uses Algorithm
						User Services (5, 6, 7, 8)
DSA-1	1112	DSA[33]	SHA-256, SHA-384, SHA-512	(2048,256)	Domain Parameter Generation	**Crypto Officer Services** (13, 24) **User Services** (none)
DSA-2				(2048,256)	Key Pair Generation	**Crypto Officer Services** (13, 24) **User Services** (none)
DSA-3			SHA-224, SHA-256 SHA-384, SHA-512	(2048,256)	Digital Signature Generation	**Crypto Officer Services** (5, 6, 7, 24) **User Services** (5, 6, 7)
DSA-4			SHA-1, SHA-224, SHA-256 SHA-384, SHA-512	(1024,160) (2048,256)	Digital Signature Verification	**Crypto Officer Services** (5, 6, 7, 24) **User Services** (5, 6, 7)
CVL-2	907	CVL –		P-224[35], P-256, P-384, P-521[35]	Shared Secret for Key Agreement Scheme	**Crypto Officer Services** (5, 6, 7) **User Services**

[33] FIPS 186-4

[35] Not used by the module.

#	CAVP Certificate	Algorithm	Mode/ Method	Key Lengths or Curves	Use	Service that uses Algorithm
		EC Diffie-Hellman Primitive[34]				(5, 6, 7)
ECDSA-1	925	ECDSA[36]		P-224, P-256, P-384, P-521	Key Pair Generation	**Crypto Officer Services** (13, 24) **User Services** (none)
ECDSA-2			SHA-224, SHA-256, SHA-384, SHA-512	P-224, P-256, P-384, P-521	Digital Signature Generation	**Crypto Officer Services** (5, 6, 7, 24) **User Services** 5, 6, 7
ECDSA-3			SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	P-192[37], P-224, P-256, P-384, P-521	Digital Signature Verification	**Crypto Officer Services** (5, 6, 7, 24) **User Services** 5, 6, 7
HMAC-3	2671	HMAC[38]	HMAC SHA-1, HMAC-SHA-1-96, HMAC SHA-224[39], HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	160, 256, 384, 512	Message Authentication	**Crypto Officer Services** (5, 6, 7, 8, 24) **User Services** (5, 6, 7, 8)

[34] SP 800-56A, Section 5.7.1.2: ECC CDH Primitive

[36] FIPS 186-4

[37] Not used in approved mode.

[38] FIPS 198-1

[39] Mode not used by module.

#	CAVP Certificate	Algorithm	Mode/ Method	Key Lengths or Curves	Use	Service that uses Algorithm
RSA-1	2215	RSA[40]	SHA-1 PKCS1 v.1.5	2048	Digital Signature Verification	**Crypto Officer Services** (5, 6, 7) **User Services** 5, 6, 7
RSA-2		RSA[41]	Random Public Exponent e	2048	Key Pair Generation	**Crypto Officer Services** (13, 24) **User Services** (none)
RSA-3			SHA-224, SHA-256, SHA-384, SHA-512 PKCS1 v.1.5	2048	Digital Signature Generation	**Crypto Officer Services** (7, 24) **User Services** (7)
RSA-4			SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	2048	Digital Signature Verification	**Crypto Officer Services** (5, 6, 7, 24) **User Services** (5, 6, 7)
SHS-3	3367	SHS[42]	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		Message Digest	**Crypto Officer Services** (5, 6, 7, 8, 11, 12, 21, 22, 24) **User Services**

[40] FIPS 186-2

[41] FIPS 186-4

[42] FIPS 180-4

#	CAVP Certificate	Algorithm	Mode/ Method	Key Lengths or Curves	Use	Service that uses Algorithm
						(5, 6, 7, 8)
TDES-3[43]	2234	Triple-DES[44]	TECB, TCBC	192	Self-tests	**Crypto Officer Services** **(24)** **User Services** none

[43] Although the certification contains Triple DES, Triple-DES is used only for self-tests in the approved mode.

[44] SP 800-67rev1

6.4 **Allowed Algorithms**

Table 23 Comware V7 Firmware - Allowed Algorithms

Algorithm	Caveat	Use	Service that uses Algorithm
Diffie-Hellman	Provides 112 bits of encryption strength.	Key establishment	**Crypto Officer Services** (5, 6, 7) **User Services** (5, 6, 7)
Elliptic Curve Diffie-Hellman Supported curves: P-256, P-384	Provides 128 or 192 bits of encryption strength.	Key establishment	**Crypto Officer Services** (5, 6, 7) **User Services** (5, 6, 7)
NDRNG[45]	A minimum of 256-bits of entropy is obtained before generating keys.	Seeding for the DRBG	**Crypto Officer Services** (none) **User Services** (none)

[45] This implementation satisfies Scenario 1(a) of IG 7.14

6.5 Non-Approved Algorithms

Table 24 Non-Approved Algorithms[46]

Algorithm	Use	Service that uses Algorithm
AES (non-compliant)	Encryption / Decryption	IKEv2, IPSEC
Camellia	Encryption / Decryption	IKEv2, IPSEC, SSHv2
DES	Encryption / Decryption	IKEv1/v2, IPSEC, SSHv1/v2, SSL
Diffie-Hellman	Key Establishment - Non-compliant less than 112 bits of encryption strength	IKEv1/v2, IPSEC, SSHv2, SSL, TLS
DSA (FIPS 186-2)	Digital Signature Generation	IKEv1/v2, IPSEC, SSHv2
DSA (FIPS 186-4)	Digital Signature Generation (security strength less than 112 bits)	IKEv1/v2, IPSEC, SSHv2
ECDSA (FIPS 186-2)	Digital Signature Generation	IKEv1/v2, IPSEC, SSHv2, SSL, TLS
ECDSA (FIPS 186-4)	Digital Signature Generation (security strength less than 112 bits)	IKEv1/v2, IPSEC, SSHv2, SSL, TLS
HMAC-MD5	Keyed Hash	IKEv1/v2, IPSEC, SSHv2, SSL, TLS

[46] Please see NIST document SP800-131Arev1 for guidance regarding the use of non FIPS-approved algorithms

MD5	Hashing	IKEv1/v2, IPSEC, SSHv2, SSL, TLS
RC2	Encryption / Decryption	SSL
RC4	Encryption / Decryption	SSL
RNG (ANSI x9.31)	Random Number Generation	Self-test
RSA (FIPS 186-2)	Asymmetric Key Generation	IKEv1/v2, IPSEC, SSHv1/v2, SSL, TLS
RSA	Key Wrapping – non-compliant less than 112 bits of encryption strength	SSHv1, SSL, TLS

7 Self-Tests

HPE Networking devices include an array of self-tests that are run during startup and during operations to prevent any secure data from being released and to insure all components are functioning correctly.

7.1 Power-On Self-Tests

The following table lists the power-on self-tests implemented by the routers. The routers perform all power-on self-tests automatically at boot. All power-on self-tests must be passed before any role can perform services. The power-on self-tests are performed prior to the initialization of the forwarding function, which prevents the security appliance from passing any data during a power-on self-test failure.

Table 25 Power-On Self-Tests

Implementation	Tests Performed
Security Appliance Software	Software/firmware Test (non-Approved RSA 2048 with SHA-256 which acts as a 256 bit EDC)
	DSA signature and verification PWCT
	ECDSA signature and verification PWCT
	ECDH KAT
	Kernel Triple-DES encryption and Triple-DES decryption KAT
	Triple-DES encryption and Triple-DES decryption KAT
	RSA signature KAT and verification KAT
	RSA signature and verification PWCT
	RSA encryption and decryption PWCT
	Kernel AES encrypt KAT and AES decrypt KAT
	AES encrypt KAT and AES decrypt KAT
	Kernel AES-GCM encrypt KAT and AES-GCM decrypt KAT
	AES-GCM encrypt KAT and AES-GCM decrypt KAT
	Kernel SHA-1 KAT
	SHA-1 KAT
	SHA224 KAT
	SHA256 KAT
	SHA384 KAT
	SHA 512 KAT

Implementation	Tests Performed
	Kernel HMAC SHA-1 KAT
	Kernel GMAC KAT
	HMAC SHA-1 KAT
	HMAC SHA224 KAT
	HMAC SHA256 KAT
	HMAC SHA384 KAT
	HMAC SHA 512 KAT
	SP800-90a CTR_DRBG KATs (Instantiate KAT, Generate KAT and Reseed KAT)

7.2 Conditional Self-Tests

The following table lists the conditional self-tests implemented by the routers. Conditional self-tests run when a router generates an ECDSA or RSA key pair and when it generates a random number.

Table 26 Conditional Self-Tests

Implementation	Tests Performed
Security Appliance Software	Pairwise consistency test for RSA
	Pairwise consistency test for DSA
	Pairwise consistency test for ECDSA
	Continuous Random Number Generator Test for the FIPS-approved SP800-90a CTR_DRBG
	SP800-90A Section 11.3 Health Tests for CTR_DRBG (Instantiate, Generate and Reseed).
	Continuous Random Number Generator Test for entropy source (NDRNG)
	Firmware Load Test (RSA PKCS#1 v1.5 2048 bits with SHA-256)

8 Delivery and Operation

8.1 Secure Delivery

To ensure no one has tampered with the goods during delivery, inspect the router physical package and check as follows:

1. Outer Package Inspection
    1) Check that the outer carton is in good condition.
    2) Check the package for a HPE Quality Seal or IPQC Seal, and ensure that it is intact.
    3) Check that the IPQC seal on the plastic bag inside the carton is intact.
    4) If any check failed, the goods shall be treated as dead-on-arrival (DOA) goods.
2. Packing List Verification

    Check against the packing list for discrepancy in material type and quantity. If any discrepancy found, the goods shall be treated as DOA goods.
3. External Visual Inspection

    Inspect the cabinet or chassis for any defects, loose connections, damages, and illegible marks. If any surface defect or material shortage found, the goods shall be treated as DOA goods.
4. Confirm Software/firmware
    1) Version verification

        To verify the software version, start the appliance, view the self-test result during startup, and use the display version command to check that the software version.

        - For the HPE FlexNetwork MSR1000, MSR2000, MSR3000 and MSR4000 Router Series, “HPE Comware, Version 7.1.045, Release R0305P08” indicates it is a FIPS 140-2 and CC certification version.

        If software loading failed or the version information is incorrect, please contact HPE for support.

    2) RSA with SHA-256 verification

        To verify that software/firmware has not been tampered, run SHA Hash command on the appliance. If the hash value is different from release notes of this software, contact HPE for support. To get release notes, please access HPE website.
5. DOA (Dead on Arrival)

    If the package is damaged, any label/seal is incorrect or tampered, stop unpacking the goods, retain the package, and report to HPE for further investigation. The damaged goods will be replaced if necessary.

8.2 Secure Operation

The rules for securely operating an HPE Networking Router in FIPS mode are:

1. Install and connect the device according to the installation and configuration guides.

2. Start the device, and enter the configuration interface.
3. Check and configure the clock.
4. By default, the device does not run in FIPS mode. Enable the device to work in FIPS mode using the **fips mode enable** command in system view. This will allow the router to internally enforce FIPS-compliance behavior, such as run power-up self-test and conditional self-test.
5. Set up username/password for crypto officer role. The password must comprise no less than 15 characters and must contain uppercase and lowercase letters, digits, and special characters.
6. Save the configurations and re-start the device.

The device works in FIPS mode after restarting:

1. Configure the security appliance to use SSHv2.

An operator can determine whether a router is in FIPS mode with the command **display fips status**. When in FIPS mode:

1. The FTP/TFTP server is disabled.
2. The Telnet server is disabled.
3. The HTTP/S server is disabled.
4. SNMP v1 and SNMP v2c are disabled. Only SNMP v3 is available.
5. The SSH server does not support SSHv1 clients
6. Generated RSA key pairs have a modulus length 2048 bits.
7. Generated ECDSA key pairs with curves P-256, P-384 and P-521.
8. SSHv2, SNMPv3, and IPsec do not support Non-FIPS approved cryptographic algorithms.

9 Physical Security Mechanism

FIPS 140-2 Security Level 2 Physical Security requirements mandate that a cryptographic module have an opaque enclosure with tamper-evident seals for doors or removable covers. HPE Networking devices include both appliance and chassis models. The tamper-evident seals and opacity shields shall be installed for the module to operate in a FIPS Approved mode of operation. All Networking devices need tamper-evident seals to meet the Physical Security requirements.

The Crypto Officer is responsible for properly placing all tamper evident labels on a device and is responsible for the securing and control of any unused seals and opacity shields. The Crypto Officer shall clean the module of any grease, dirt, or oil before applying the tamper-evident labels or opacity shields. The Crypto Officer is also responsible for the direct control and observation of any changes to the modules such as reconfigurations where the tamper-evident labels or opacity shields are removed or installed to ensure the security of the module is maintained during such changes and the module is returned to a FIPS approved state. The security labels recommended for FIPS 140-2 compliance are provided in the FIPS Kit. These security labels are very fragile and cannot be removed without clear signs of damage to the labels.

MSR1000 series and MSR2000 Series

Unit	**Opacity Kit – Description**	**Opacity kit – Part Number**
HPE FlexNetwork MSR1000 Router	HPE FlexNetwork MSR2003 Opacity Shield Kit	JG598A
HPE FlexNetwork MSR2000 AC Router	HPE FlexNetwork MSR2003 Opacity Shield Kit	JG598A

MSR3000 series

Unit	**Opacity Kit – Description**	**Opacity kit – Part Number**
HPE FlexNetwork MSR3012 Router	HPE FlexNetwork MSR3012 Opacity Shield Kit	JG599A
HPE FlexNetwork MSR3044 Router	HPE FlexNetwork MSR3044 Opacity Shield Kit	JG600A
HPE FlexNetwork MSR3064 Router	HPE FlexNetwork MSR3064 Opacity Shield Kit	JG601A

MSR4000 series

Unit	**Opacity Kit – Description**	**Opacity kit – Part Number**
HPE FlexNetwork MSR4060 Router Chassis	HPE FlexNetwork MSR4060 Opacity Shield Kit	JG602A
HPE FlexNetwork MSR4080 Router Chassis	HPE FlexNetwork MSR4080 Opacity Shield Kit	JG603A

All units use the same tamper evidence label kits:

Label Kit – Description	**Label Kit - Part Number**
HPE 12mm x 60mm Tamper-Evidence (30) Labels	JG585A
HPE 12mm x 60mm Tamper-Evidence (100) Labels	JG586A

Each modular router is entirely encased by a thick steel chassis. Power cable connection and a power switch are provided on the power supplies.

Use the procedure described in FIPS enclosure install instruction to apply tamper evident labels to the router.

The Crypto Officer should inspect the tamper evident labels periodically to verify they are intact and the serial numbers on the applied tamper evident labels match the records in the security log. If evidence of tampering is found with the TELs, the module must immediately be powered down and all administrators must be made aware of a physical security breach in compliance the local site policies and procedures for dealing with this type of incident.

10 Mitigation of Other Attacks

The Security appliances do not claim to mitigate any attacks in a FIPS approved mode of operation.

11 Documentation References

11.1 Obtaining documentation

You can access the HPE Networking products page: http://h17007.www1.hp.com/us/en/ , where you can obtain the up-to-date documents of HPE Routers and Switches, such as datasheet, installation manual, configuration guide, command reference, and so on.

11.2 Technical support

For technical or sales related question please refer to the contacts list on the HPE website: http://www.HP.com.

The actual support website is:

http://www8.hp.com/us/en/support-drivers.html